BTopenworld Business Broadband

Intelligent Gateway 1800
User Guide

Notice to Users

2WIRE PROVIDES NO WARRANTY WITH REGARD TO THIS MANUAL, THE SOFTWARE, OR OTHER INFORMATION CONTAINED HEREIN AND HEREBY EXPRESSLY DISCLAIMS ANY IMPLIED WARRANTIES OF MERCHANTABILITY OR FITNESS FOR ANY PARTICULAR PURPOSE WITH REGARD TO THIS MANUAL, THE SOFTWARE, OR SUCH OTHER INFORMATION, IN NO EVENT SHALL 2WIRE, INC. BE LIABLE FOR ANY INCIDENTAL, CONSEQUENTIAL, OR SPECIAL DAMAGES, WHETHER BASED ON TORT, CONTRACT, OR OTHERWISE, ARISING OUT OF OR IN CONNECTION WITH THIS MANUAL, THE SOFTWARE, OR OTHER INFORMATION CONTAINED HEREIN OR THE USE THEREOF.

2Wire, Inc. reserves the right to make any modification to this manual or the information contained herein at any time without notice. The software described herein is governed by the terms of a separate user license agreement.

Updates and additions to software may require an additional charge. Subscriptions to online service providers may require a fee and credit card information. Financial services may require prior arrangements with participating financial institutions.

Owner's Record

The serial number is located on the bottom of your Intelligent Gateway. Record the serial number in the space provided here and refer to it when you call Customer Care.

Serial Number:__________________________

Safety Information

- Use of an alternative power supply may damage the Intelligent Gateway, and will invalidate the approval that accompanies the Intelligent Gateway.
- To prevent fire or shock hazard, do not expose your Intelligent Gateway to rain or moisture.
- To avoid electrical shock, do not open the Intelligent Gateway. Refer servicing to qualified personnel only.
- An electrical storm could damage the Intelligent Gateway. To avoid this possibility, disconnect the Intelligent Gateway from the mains power and telephone line during an electrical storm.
- Never install telephone sockets in wet locations unless the socket is specifically designed for wet locations.
- Never touch uninsulated telephone wire or terminals unless the telephone line has been disconnected at the network interface.
- Use caution when installing or modifying cable or telephone lines.
- Avoid using your modem during an electrical storm.
- Do not use your modem or a telephone to report a gas leak in the vicinity of the leak.
- Install your Intelligent Gateway within 1830mm of a mains socket. Use caution when laying out the cable to avoid hazard to people walking near or using the equipment.

Contents

To display the Table of Contents in the left-hand pane, click the Window menu and select Bookmarks.

Networking Technology Overview

Step 1: Getting Started

Step 2: Connect Your First Computer to the Intelligent Gateway

Step 3: Install the Intelligent Gateway Software

Step 4: Add Computers to the Network

Using the Intelligent Gateway Network

Firewall Monitor

Access Controls

Sharing Files and Printers

Networking Technology Overview

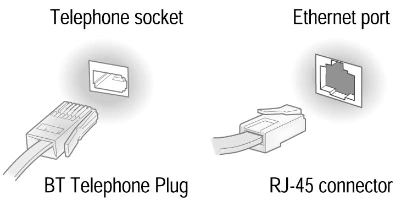
When two or more computers are connected so they can “talk” with each other, a computer network is established. Individual users can now connect to Web servers worldwide through the Internet, a global computer network. A local area network (LAN) enables computer users in a business or household to share files without trading disks, and share peripherals such as printers and external drives.

With the Intelligent Gateway, computers on a LAN can share a connection to the Internet. Several technologies are available to connect or “network” computers. These technologies include:

- Ethernet
- Universal Serial Bus (USB)
- HomePNA
- Wireless

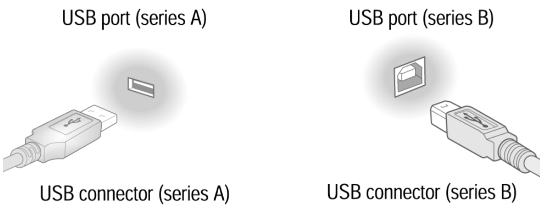
Ethernet

Ethernet is a technology that allows you to create a network using special wiring (Category 5 cable), such as the dark gray cable included with the Intelligent Gateway. Many computers are shipped with a built-in Ethernet adapter. If you have a computer with an Ethernet adapter, you can use Ethernet cable to connect the Ethernet connection socket on the computer to any available local Ethernet port on the Intelligent Gateway. You can identify an Ethernet connection socket by its rectangular shape and size, which is slightly larger than a standard telephone socket.

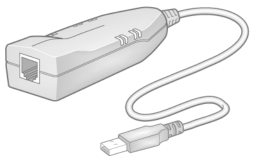


USB

Most computers manufactured in the last few years come with USB connections. USB ports, which are small and rectangular, are typically located on the back of the computer and are marked with the USB symbol (⭠). Use a USB connection for a computer that is in close proximity to the Intelligent Gateway.

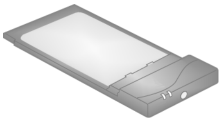


Home Phoneline Networking (HomePNA)



The Intelligent Gateway supports the Home Phoneline Networking Alliance protocol. HomePNA technology lets you connect computers in different rooms using your home's existing telephone wiring. To create a home phoneline network, you need an external HomePNA adapter for each additional computer you connect to the network using HomePNA. These devices make it possible to connect each additional computer through the phoneline. Use HomePNA for connecting computers to your Intelligent Gateway if it is used in a home environment.

Wireless



The Intelligent Gateway supports 802.11b wireless networking, which uses radio waves to connect your computers to your network. Each computer on your network will need an adapter to work with the system. Two types of adapter are common: a PC card (commonly used for laptop computers) and a USB adapter (commonly used for desktop computers). Use wireless technology for networking computers that are not accessible with physical wiring or require mobility, such as laptop computers.

Intelligent Gateway

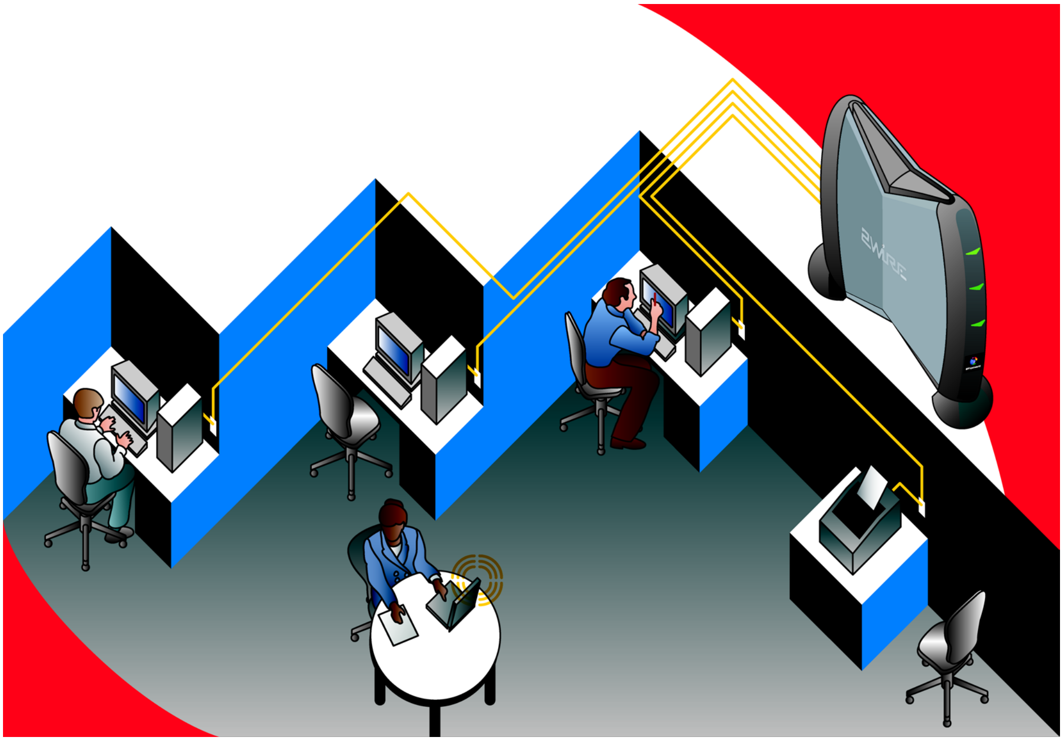
The Intelligent Gateway makes it possible to create a LAN using any or all of the technologies described above. All Intelligent Gateway network interfaces are completely functional at the same time. This means that you can have different computers simultaneously connecting with each other using Ethernet, USB, HPNA, and wireless (optional wireless expansion card required). By enabling you to connect all of the computers in your small business or home office, the Intelligent Gateway provides you with the benefits of networking, including the ability to share one Internet connection among all the computers and computer users at your location.

The Intelligent Gateway offers the following features:

- Delivers rich content from the Internet, distributing it to multiple simultaneous users.
- Provides shared usage of files and printers among users.
- Enables high-speed, continuous Internet access to the computers on your network—while keeping your confidential files safe from Internet hackers. Intelligent Gateway has a built-in firewall, with stateful packet inspection, to keep your network safe.
- Allows users to connect to the local network securely through the Internet anywhere in the world.
- Provides a 4-port 10/100 Ethernet switch allowing users to create a larger, faster networking environment.

Plan your network

The following diagram shows a recommended location for the Intelligent Gateway and your computers.



Place the Intelligent Gateway in a visible, easily accessible location near the power mains, telephone socket, and a computer. If your office computer has Windows 98, ME, 2000, or XP, we recommend connecting it via Ethernet. For two computers, consider using USB and Ethernet. If you have multiple computers requiring Ethernet, you can use any of the available local Ethernet ports on the Intelligent Gateway to connect the computers to the Intelligent Gateway.

Step 1 *Getting Started*

First: Remove or disable conflicting applications

Applications that enable a computer to share its Internet connection (often called Internet sharing software) and PC based firewall applications typically interfere with the Intelligent Gateway and should be removed or disabled before you install the Intelligent Gateway. The Intelligent Gateway provides all of the same features as the products listed below so you don't need to worry about losing Internet sharing and security capabilities.

If you have any of the following (or similar) applications installed on your computers, remove or disable them according to the manufacturer's instructions before proceeding.

Internet sharing applications such as...	Proxy software such as...	Security software such as...
• 3Com HomeClick • Microsoft Internet Connection Sharing • Intel Anypoint ISS	• WinGate • Sygate	• Norton Internet Security • McAfee • Black Ice • Zone Alarm

Second: Check your computer's system and browser requirements

Verify that your computers meet the following minimum requirements:

System Requirements

Windows:

- Windows 98, 98SE, Windows ME, Windows NT 4.0 with Service Pack 6, Windows 2000, or Windows XP
- At least 32 MB of RAM
- At least one computer with CD-ROM
- 5 MB of available hard disk space for Intelligent Gateway software
- Available Ethernet or USB port

Macintosh:

- Mac OS 8.6 or higher (USB connectivity is not supported for Mac OS 10.0 or 10.1)
- At least 32 MB of RAM
- At least one computer with CD-ROM
- 10 MB of available hard disk space for Intelligent Gateway software
- Available Ethernet port

Browser Requirements

Windows: Microsoft Internet Explorer 5.0 or higher (Internet Explorer 6.0 is included on the Intelligent Gateway Setup Wizard CD) **or** Netscape Navigator 4.7 or higher.

Macintosh: Microsoft Internet Explorer 5.0 **or** Netscape 4.74 or higher.

Third: Install your ADSL Filter

Because telephony and DSL signals are carried between the exchange and your office over the same cable, filters are needed to split the signals within your office. By separating the computer data and voice signals, the ADSL Filter enables you to use your telephone and broadband services simultaneously. Install one ADSL Filter for each telephony connection, including such devices as answering machines, fax machines, point of sale terminals, and PSTN dial up modems.

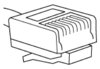
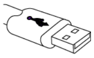
You must install an ADSL Filter for each telephone or telephony device that shares the same line as your ADSL modem. To do so:

- Disconnect your telephone/other telephony equipment from the wall socket
- Connect the “tail” of the ADSL Filter into the wall socket
- Connect the line cord from your phone or other equipment into the ADSL Filter socket marked **PHONE**
- Note that the socket marked **ADSL MODEM** is unused at this stage
- Repeat this procedure for your other telephones/telephony equipment
- Unused sockets do not need an ADSL Filter installed

Step 2 Connect Your First Computer to the Intelligent Gateway

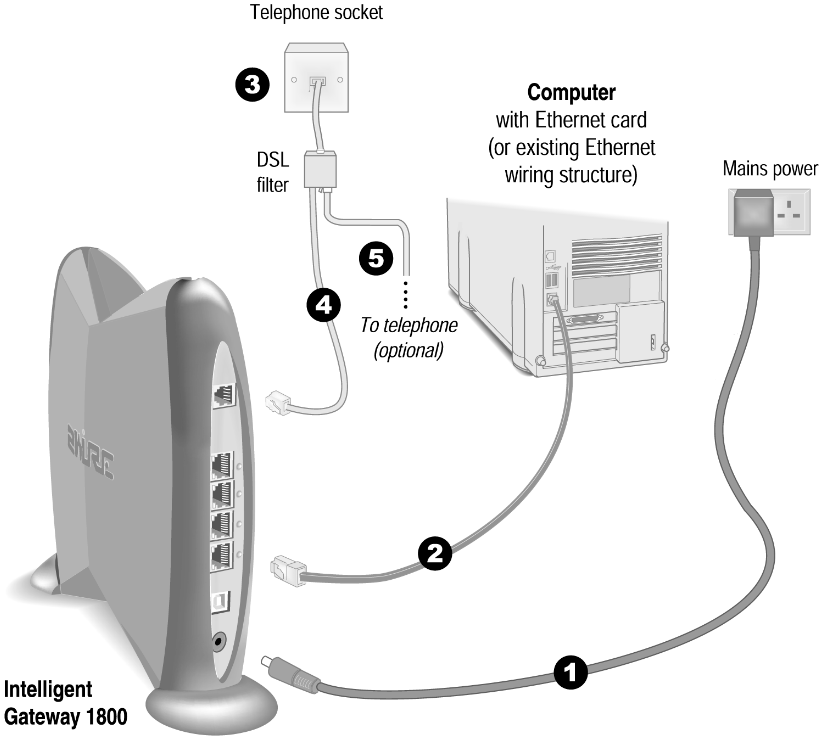
Choose a computer and connection type

The first computer you connect to your local network is used to configure the Intelligent Gateway for proper operation, and should be located in the same room as the Intelligent Gateway. Choose one of the following methods to connect your first computer to the Intelligent Gateway. Save and close all open programs before you begin connecting your Intelligent Gateway.

	Connection Type	Go to...
	**Ethernet** *Requires:* A computer with an Ethernet port. *Recommended for:* Primary computer in the same room as the Intelligent Gateway.	**page 7**
	**USB** *Requires:* A computer with an available USB port. See the USB connection option for exceptions. *Recommended for:* Primary computer in the same room as the Intelligent Gateway.	**page 8**

Ethernet Connection

Requires a computer with an Ethernet port



1. Connect the provided AC power adapter from the Intelligent Gateway's **POWER** port to an electrical outlet. The green **POWER** light on the front of the Intelligent Gateway should light up.
2. Connect the provided Ethernet cable from any available **LOCAL ETHENET** port on the Intelligent Gateway to your computer's Ethernet port.
3. Connect the provided ADSL Filter to the telephone socket.
4. Connect the provided telephone cable from the **PHONE LINE** port on the Intelligent Gateway to the **ADSL MODEM** socket on the ADSL Filter.

   This connects the internal DSL modem of the Intelligent Gateway to your DSL service provider. If you have been using an external DSL modem, disconnect it as you will no longer need it.
5. (Optional). If you had a telephone connected to the telephone socket, you can reconnect it to the **PHONE** port on the ADSL Filter.

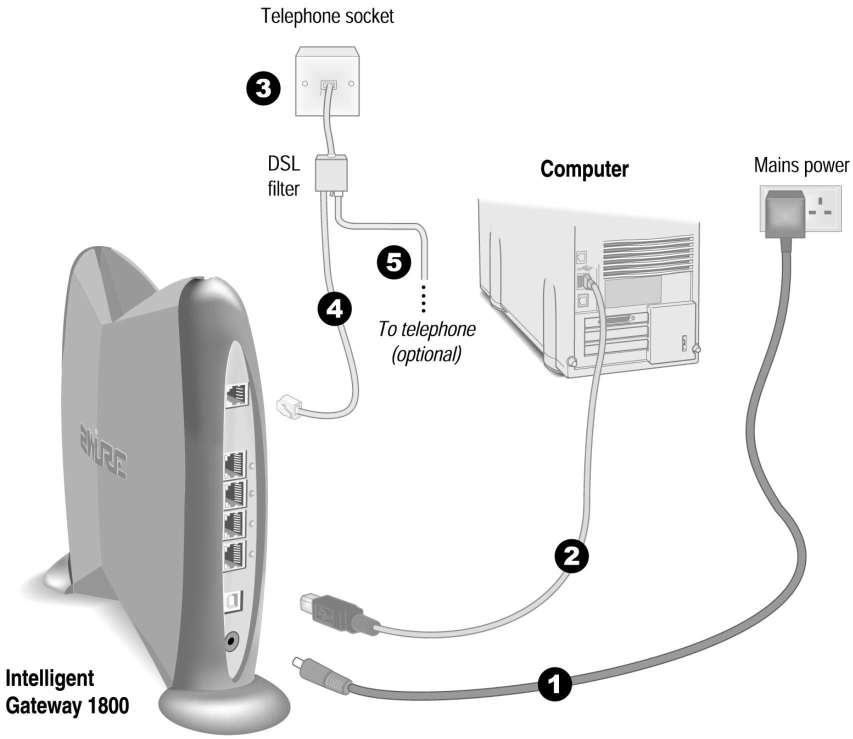
Check your connections

Power-on your computer. When your computer is fully powered-up, verify the **POWER** and **LOCAL NETWORK** indicator lights on the front of the Intelligent Gateway are green. If they are not, see "Diagnosing connection problems" on page 110. *The **BROADBAND LINK** indicator light will not turn green until the Intelligent Gateway software has been installed and an Internet connection has been established.*

Continue from here to Step 3 "Install the Intelligent Gateway Software" on page 12.

USB Connection

Requires a computer with an available USB port. Refer to the note below for exceptions.



Note: *Only one Windows or Macintosh computer can be directly connected to the Intelligent Gateway using the USB connection. Intelligent Gateway USB connectivity is NOT available for Macintosh OS earlier than 8.6, Mac OS 10.0, Mac OS 10.1, Windows 95, Window 95 OSR2, or Windows NT. Additional computers may be added to the network using connection options such as Ethernet.*

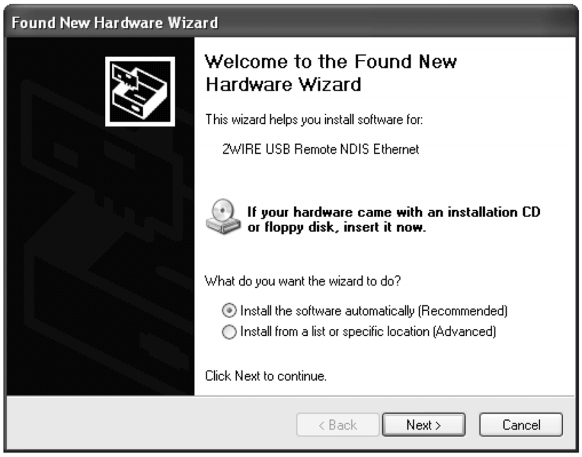
1. Connect the provided AC power adapter from the Intelligent Gateway's **POWER** port to an electrical outlet. The green **POWER** light on the front of the Intelligent Gateway should light up.
2. Connect the provided USB cable from the **PC** port on the Intelligent Gateway to the USB port on your computer. The gray end fits into the Intelligent Gateway and the beige end goes to your PC.
3. Connect the provided ADSL Filter to the telephone socket.
4. Connect the provided telephone cable from the **PHONE LINE** port on the Intelligent Gateway to the **ADSL MODEM** port on the ADSL Filter.

   This connects the internal DSL modem of the Intelligent Gateway to your DSL service provider. If you have been using an external DSL modem, disconnect it as you will no longer need it.
5. (Optional). If you had a telephone connected to the telephone socket, you can reconnect it to the **PHONE** port on the ADSL Filter.

Install the Intelligent Gateway USB driver — Windows PC

Before installing your Intelligent Gateway software, you must install the Intelligent Gateway USB driver on your computer. The following screens show the installation under Windows XP and may vary somewhat on Windows 98, Windows ME, and Windows 2000.

1. Power on your computer. When the Found New Hardware Wizard window opens, make sure that **Install the software automatically (Recommended)** is selected and click **Next** to continue.



Found New Hardware Wizard

Welcome to the Found New Hardware Wizard

This wizard helps you install software for:

2WIRE USB Remote NDIS Ethernet

If your hardware came with an installation CD or floppy disk, insert it now.

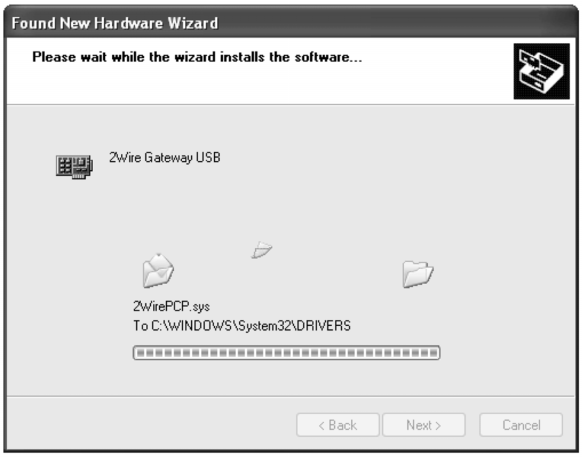
What do you want the wizard to do?

● Install the software automatically (Recommended)

○ Install from a list or specific location (Advanced)

Click Next to continue.

2. The driver installs.



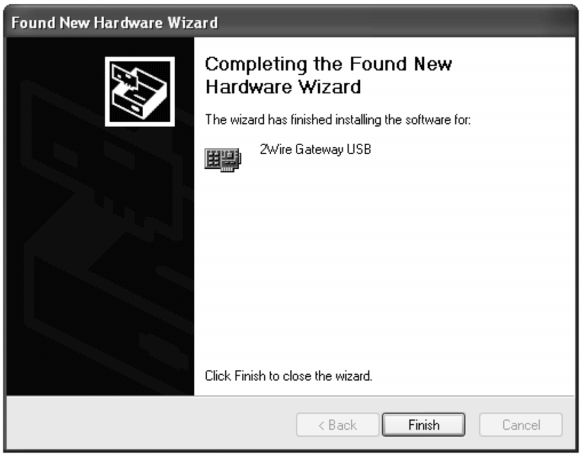
Found New Hardware Wizard

Please wait while the wizard installs the software...

2Wire Gateway USB

2WirePCP.sys
To C:\WINDOWS\System32\DRIVERS

3. Click **Finish** to complete the installation.



Found New Hardware Wizard

Completing the Found New Hardware Wizard

The wizard has finished installing the software for:

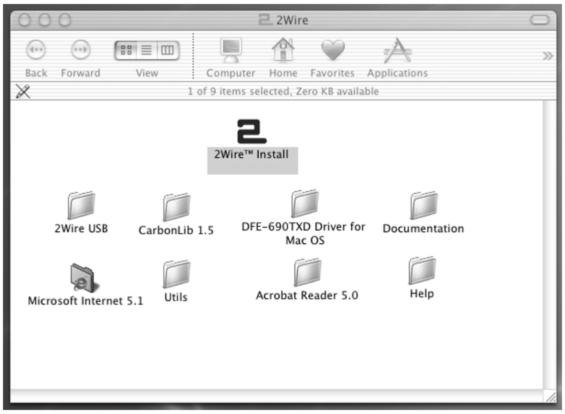
2Wire Gateway USB

Click Finish to close the wizard.

Install the Intelligent Gateway USB driver — Macintosh

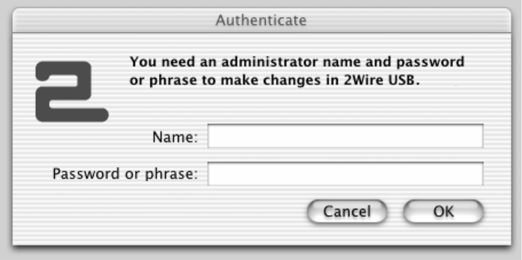
Before installing your Intelligent Gateway software, you must install the Intelligent Gateway USB driver on your computer. The following screens show the installation under Macintosh OS 10.2 and may vary somewhat on Macintosh OS 8.6 to 9.X.

1. Power on your computer.
2. Insert the Intelligent Gateway Setup Wizard CD in your computer's CD-ROM drive.
3. Double-click the 2Wire USB folder to install the driver.



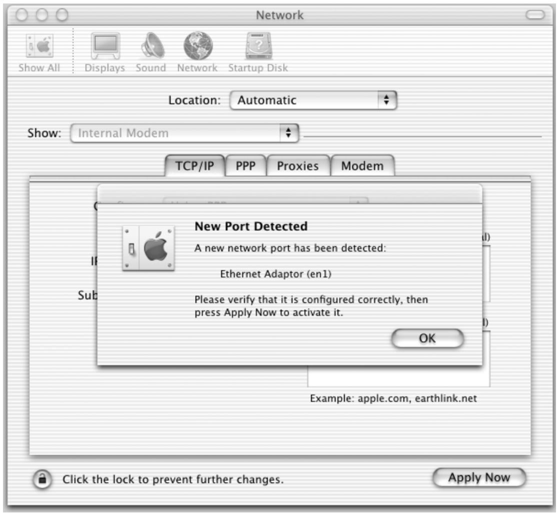
1 of 9 items selected, Zero KB available

4. If you have set up an administrator name and password, the Authenticate screen opens. Enter your administrator name and password and click **OK**.
5. Follow the on-screen instructions. When the driver installation is complete, you will be prompted to restart your computer.



You need an administrator name and password or phrase to make changes in 2Wire USB.

6. After your computer restarts, connect a USB cable from your Macintosh computer to the Intelligent Gateway USB port.
7. Establish your connection. Open the network Control Panel and select the **Apple icon>System Preferences...>Network**.



Location: Automatic

Show: Internal Modem

New Port Detected

A new network port has been detected:

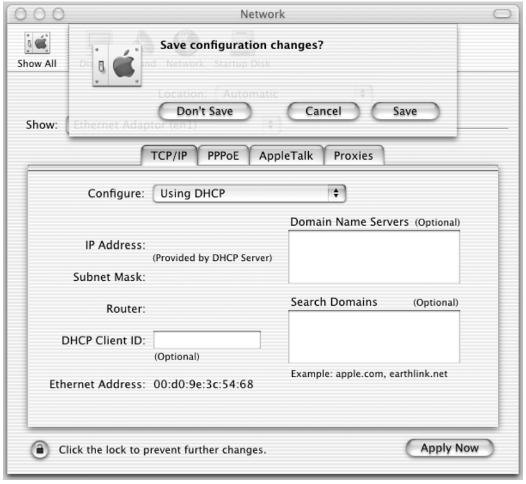
Ethernet Adaptor (en1)

Please verify that it is configured correctly, then press Apply Now to activate it.

Example: apple.com, earthlink.net

Click the lock to prevent further changes.

8. Verify that **Ethernet Adaptor (en1)** is selected in the Show field. If it is not, select it from the pull-down menu. When the New Port Detected message displays, click **OK**.
9. Click **Save** to complete your installation.



Network

Save configuration changes?

Location: Automatic

Show: Ethernet Adaptor (en1)

Configure: Using DHCP

IP Address: (Provided by DHCP Server)

Subnet Mask:

Router:

DHCP Client ID: (Optional)

Ethernet Address: 00:d0:9e:3c:54:68

Domain Name Servers (Optional)

Search Domains (Optional)

Example: apple.com, earthlink.net

Click the lock to prevent further changes.

Note: *Your Macintosh computer automatically assigns the name "(en1)" to the Intelligent Gateway USB port. If your computer has more than one Ethernet-type network device installed, the USB port may be named "(en2)" or higher.*

Check your connections

Power-on your computer. When your computer is fully powered-up, verify the **POWER** and **LOCAL NETWORK** indicator lights on the front of the Intelligent Gateway are green. If they are not, see "Diagnosing connection problems" on page 110. *The **BROADBAND LINK** indicator light will not turn green until the Intelligent Gateway software has been installed and an Internet connection has been established.*

Continue from here to Step 3 "Install the Intelligent Gateway Software" on page 12.

Step 3 Install the Intelligent Gateway Software

Before installing the Intelligent Gateway software, it is very important that you disable any conflicting applications such as firewall and file- and printer-sharing applications. See Step 1, "Getting Started."

BT Openworld Pay-As-You-Go Dial Up Connection Option

Before installing the Intelligent Gateway software, please make sure that you have your username, password, and email address that were provided in your Welcome Letter and via email.

When the Setup Wizard CD starts, you will be guided through the BT Openworld Plug & Go installation, which gives you the option of installing Internet Explorer, Outlook Express, and Windows Media Player on your computer. You will be prompted for information that enables BT Openworld to automatically configure your mail account in Outlook Express and set up your default home page in Internet Explorer.

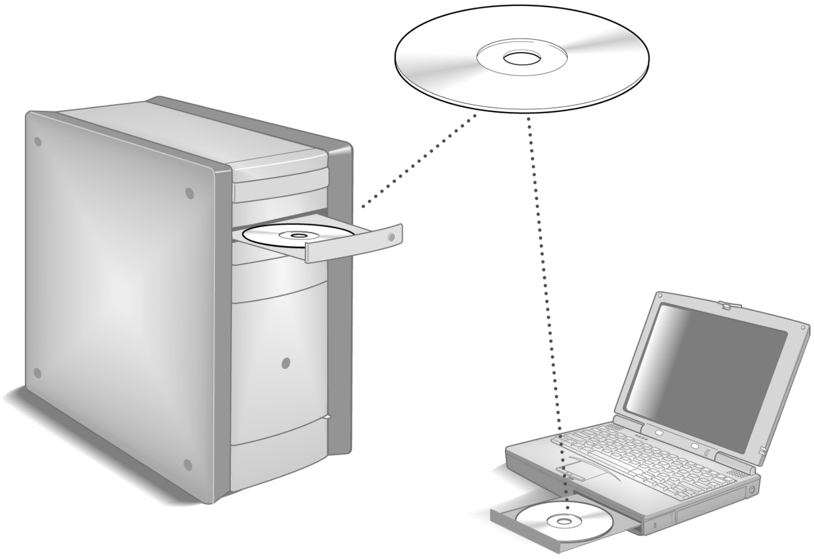
You will also be given the option of installing a Pay-As-You-Go dial-up connection, which will allow you to connect to the Internet if broadband service is not available. To use the dial-up service, your computer must be connected to your telephone line via a dial-up modem, and during set up you will be prompted to select which modem you want to use. You can install the dial-up connection on each PC that has a modem and that is connected to the network.

IMPORTANT: *When you connect a dial-up modem to the same line that is being used for your broadband service, you MUST use an ADSL Filter.*

If you do not want to install the dial-up connection during set up, you can install it at a later time by navigating to the PAYG folder on the Setup Wizard CD and double-clicking the SetupPAYG.exe file.

To use the dial-up connection, double-click the BT Openworld Connect PAYG desktop icon, enter your password (if prompted), and connect. Make note of your username and password so that this information is readily available if you need it. Your username for PAYG is your email address, and your password is provided in your Welcome Letter and via email. Please note that you will be charged at the usual Pay-As-You-Go rates when you use this connection.

Installing the Intelligent Gateway Setup Wizard on Windows PCs



Note: *Close all programs before running the Intelligent Gateway Setup Wizard. The Intelligent Gateway software must be installed on all computers in your network.*

Place the *Intelligent Gateway Setup Wizard* CD in the CD-ROM drive of your computer and follow the onscreen instructions. It may take up to one full minute for the Setup Wizard to start.

Starting the Setup Wizard manually on Windows PCs

After one minute, if the Setup Wizard does not run automatically, follow these steps:

1. Double-click the **My Computer** icon located on the desktop.
2. Double-click the icon that corresponds to your CD-ROM drive, then double-click **Setup.exe**.
3. Follow the onscreen instructions.
4. After the software installation is complete, your Intelligent Gateway is ready to use ADSL service and the **POWER**, **LOCAL NETWORK**, and **BROADBAND LINK** LEDs should be green.

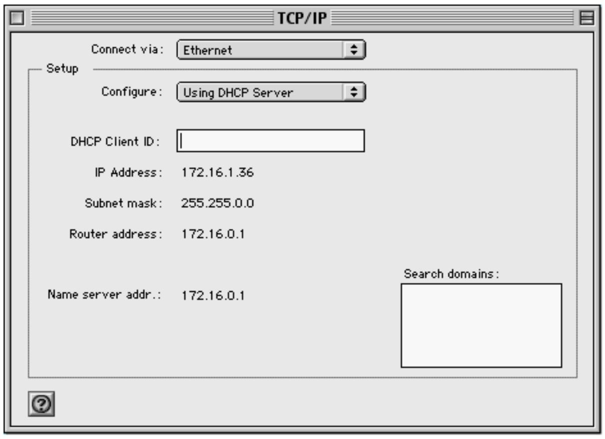
Note: *Refer to the "Using the Intelligent Gateway Network" chapter for information about the computers on your network.*

Configuring the Intelligent Gateway on Macintosh computers

Refer to the “Welcome Letter” that was included in you Intelligent Gateway package. It provides the key code you will need to configure the Intelligent Gateway on your Macintosh computer.

Macintosh 8.6 and 9.x

1. Click the Apple menu and select **Control Panel>TCP/IP**. The TCP/IP menu opens.
2. From the **Connect via** dropdown, select the method by which the Intelligent Gateway will connect to your computer (Ethernet, PC Port, or wireless).
3. From the **Configure** dropdown, select **Using DHCP Server**.
4. Exit the TCP/IP menu. Click **Yes** when prompted to save changes.



TCP/IP

Connect via: Ethernet

Setup

Configure: Using DHCP Server

DHCP Client ID:

IP Address: 172.16.1.36

Subnet mask: 255.255.0.0

Router address: 172.16.0.1

Name server addr.: 172.16.0.1

Search domains:

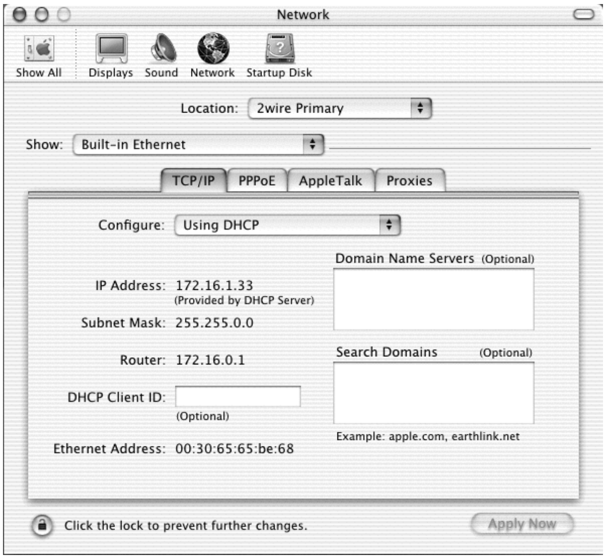
5. After the software installation is complete, your Intelligent Gateway is ready to use ADSL service and the **POWER**, **LOCAL NETWORK**, and **BROADBAND LINK** LEDs should be green.

Note: *Refer to the “Using the Intelligent Gateway Network” chapter for information about the computers on your network.*

Macintosh OS X

1. Click the Apple menu and select **System Preference>Network**.
2. From the **Show** dropdown, select the method by which the Intelligent Gateway will connect to your computer (Built-in Ethernet, PC Port, or wireless).
3. Click the TCP/IP tab.
4. From the **Configure** dropdown, select **Using DHCP**.
5. Click **Apply Now**.
6. After the software installation is complete, your Intelligent Gateway is ready to use ADSL service and the **POWER**, **LOCAL NETWORK**, and **BROADBAND LINK** LEDs should be green.

Note: *Refer to the “Using the Intelligent Gateway Network” chapter for information about the computers on your network.*



Location: 2wire Primary

Show: Built-in Ethernet

Configure: Using DHCP

Domain Name Servers (Optional)

IP Address: 172.16.1.33 (Provided by DHCP Server)

Subnet Mask: 255.255.0.0

Router: 172.16.0.1

Search Domains (Optional)

DHCP Client ID: (Optional)

Example: apple.com, earthlink.net

Ethernet Address: 00:30:65:65:be:68

Click the lock to prevent further changes.

Step 4 Add Computers to the Network

Choose a computer and connection type

After your first computer is connected to the Intelligent Gateway and your Internet connection has been established, it is time to connect the other computers to the network.

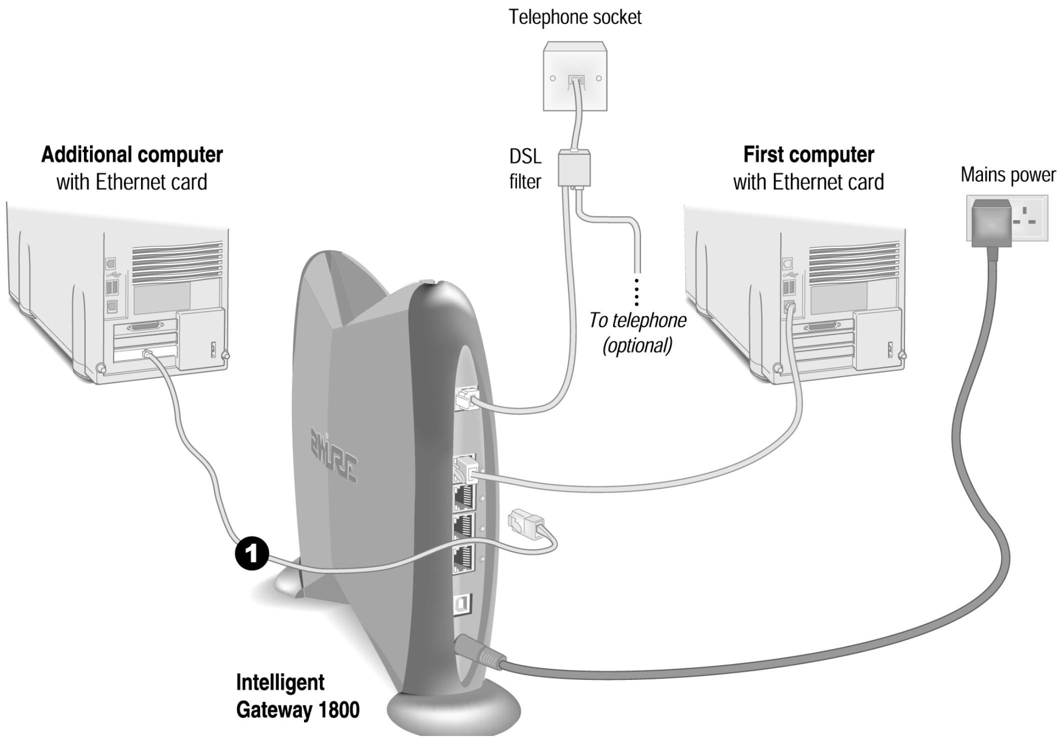
Use any or all of the following methods to connect additional computers to your network:

Connection Type	Go to...
Ethernet Requires a computer with an Ethernet port. *Recommended for small office environments using Ethernet (Category 5) wiring.*	**page 16**
USB Requires a computer with an available USB port. See the USB connection option for exceptions.	**page 17**
Home phoneline networking (HomePNA) Requires a computer with a HomePNA port or an external HomePNA adapter such as the PC Port.	**page 18**
Wireless Requires a computer with a Wi-Fi compliant (802.11b) wireless network adapter installed and a 2Wire Wireless PC Card* installed in the Intelligent Gateway. Wireless adapters are purchased separately from the Intelligent Gateway. *Recommended for mobile computers such as laptops.*	**page 20**

* *You must use a 2Wire Wireless PC Card to convert your Intelligent Gateway into a wireless broadband router. Other wireless cards are not supported.*

Ethernet Connection

Requires a computer with an Ethernet port

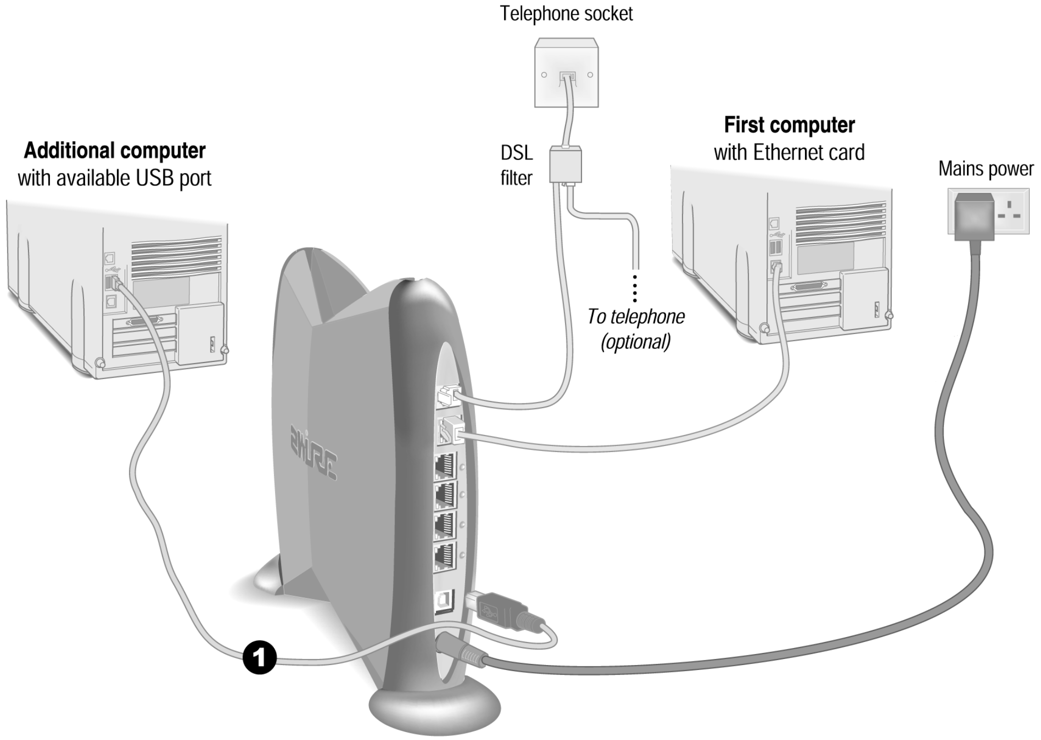


1. Connect an Ethernet cable from any available **LOCAL ETHERNET** port on the Intelligent Gateway to your computer's Ethernet port.

Repeat Step 3 "Install the Intelligent Gateway Software" on page 12.

USB Connection

Requires a computer with an available USB port. Refer to the note below for exceptions.



Note: *Only one Windows or Macintosh computer can be directly connected to the Intelligent Gateway using the USB connection. Intelligent Gateway USB connectivity is NOT available for Macintosh OS earlier than 8.6, Mac OS 10.0, Mac OS 10.1, Windows 95, Window 95 OSR2, or Windows NT. Additional computers may be added to the network using connection options such as Ethernet.*

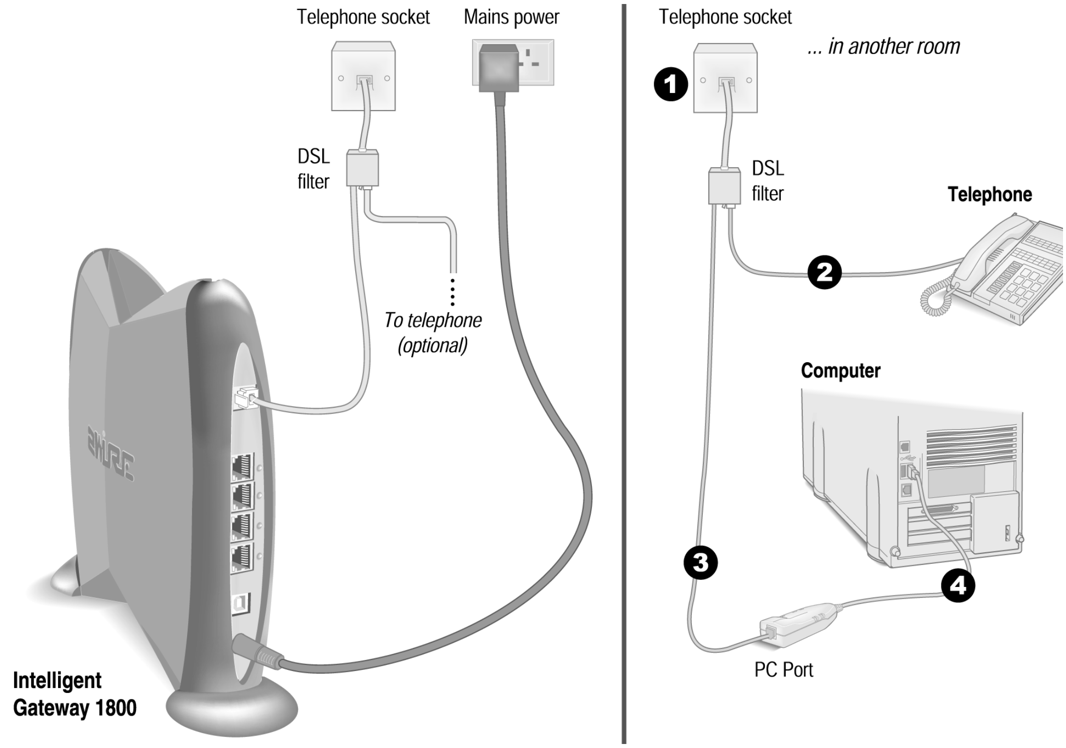
1. Connect the USB cable from the **PC** port on the Intelligent Gateway to the USB port on your computer.

Before installing your Intelligent Gateway software on this computer, you must install a USB driver. Detailed instructions for installing USB drivers begins on page 8.

Repeat Step 3 "Install the Intelligent Gateway Software" on page 12.

Home Phoneline Networking (HomePNA) Connection

If a telephone is located in the same room in which the PC Port will be installed



Computers connected with HomePNA access the Internet connection on the Intelligent Gateway and other computers on the network using existing telephone wiring. You will need one PC Port for each computer that you are connecting through HomePNA.

1. Connect the provided ADSL Filter to the telephone socket.
2. Connect the standard telephone cable from the **PHONE** port on the ADSL Filter to the telephone.
3. Connect one end of the provided RJ-11/RJ-11 telephone cable (the short adapter cable with the same type of plug on both ends) to the **ADSL MODEM** port on the ADSL Filter, and the other end to the PC Port.
4. Insert the PC Port into the USB port on your computer.

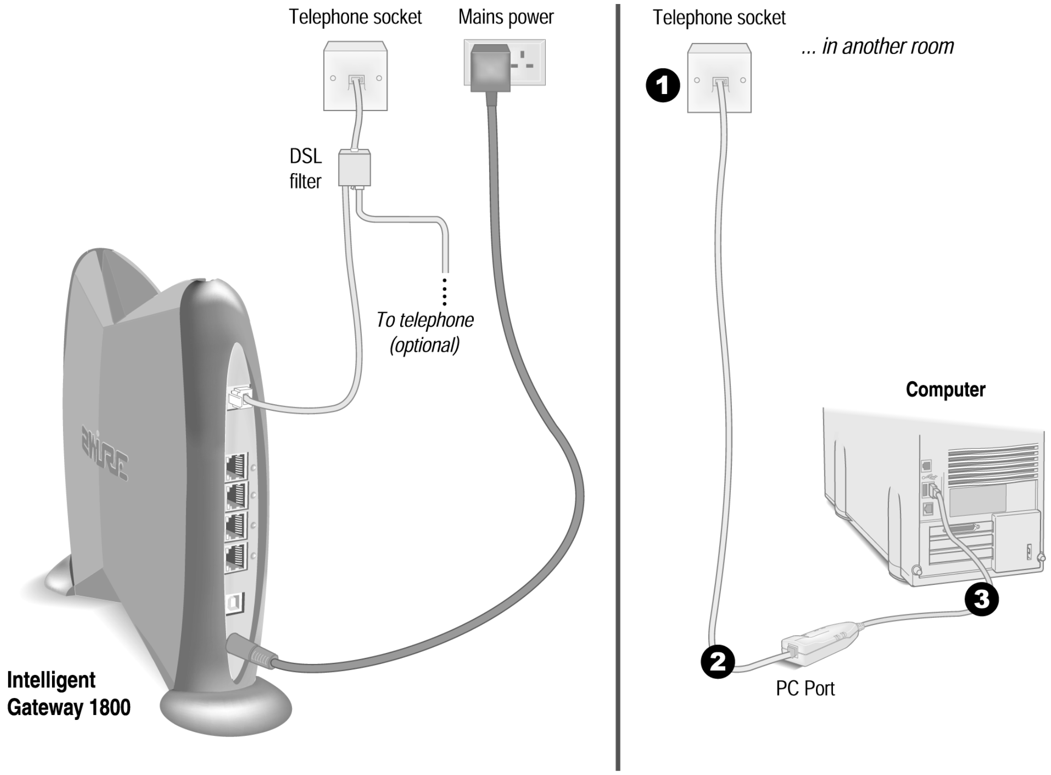
Install the PC Port Driver

- Power on the computer. Windows recognizes the PC Port and automatically launches the Add New Hardware Wizard.
- Select **Specify the location of the driver (Advanced)** and click **Next** to continue.
- Insert the PC Port CD and wait for the CD to start up. Select **Removable Media (Floppy, CD-ROM...)** and click **Next** to continue.
- Windows is now ready to load the network driver. Click **Next** to continue.
- Click **Finish**. Windows may take several minutes to complete the driver installation as it copies the files on to your computer.
- Click **Yes** to restart the computer. If your System Settings Change window does not appear, restart your computer: from the Start menu, select **Shut Down > Restart > OK**.

After your PC Port and PC Port driver are successfully installed, repeat Step 3 "Install the Intelligent Gateway Software" on page 12.

Home Phoneline Networking (HomePNA) Connection

If there is no telephone located in the room in which PC Port will be installed



Computers connected with HomePNA access the Internet connection on the Intelligent Gateway and other computers on the network using existing telephone wiring. You will need one PC Port for each computer that you are connecting through HomePNA. If you are connecting a PC to the network and do not need a telephone to be connected at the same location, use the long telephone cable provided with the PC Port.

1. Connect the end of the telephone cable with the standard telephone plug into the telephone socket.
2. Connect the other end of the telephone cable into the PC Port.
3. Insert the PC Port into the USB port on your computer.

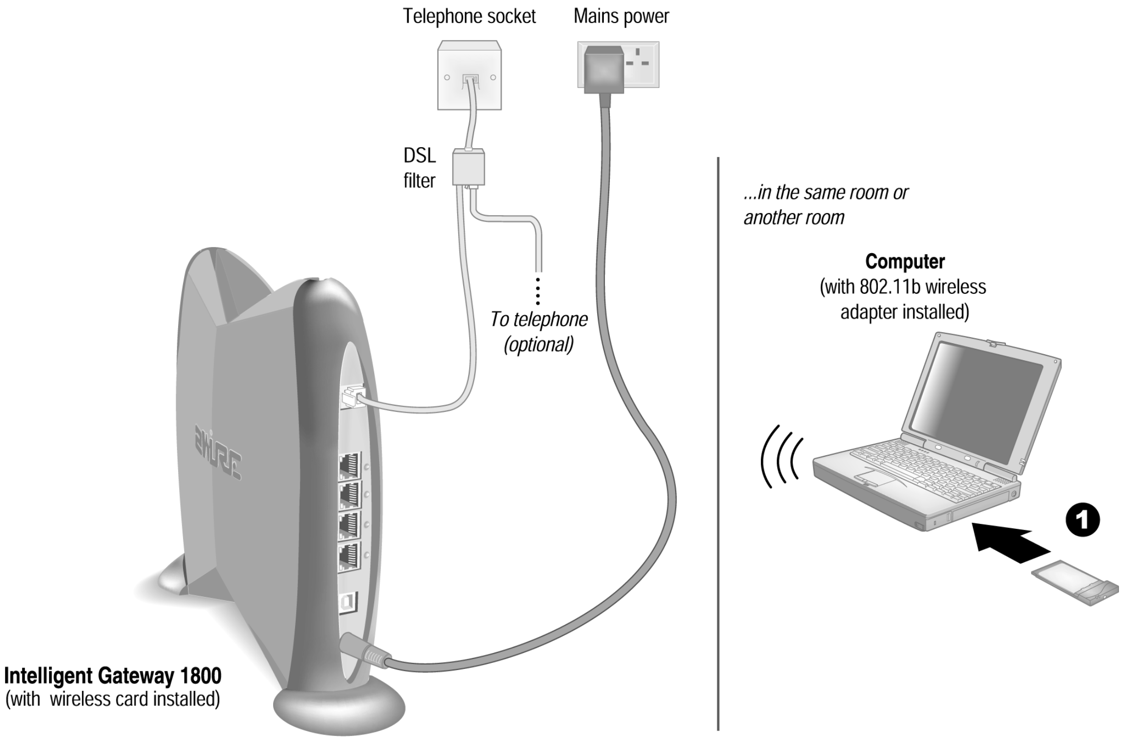
Install the PC Port Driver

- Power on the computer. Windows recognizes the PC Port and automatically launches the Add New Hardware Wizard.
- Select **Specify the location of the driver (Advanced)** and click **Next** to continue.
- Insert the PC Port CD and wait for the CD to start up. Select **Removable Media (Floppy, CD-ROM...)** and click **Next** to continue.
- Windows is now ready to load the network driver. Click **Next** to continue.
- Click **Finish**. Windows may take several minutes to complete the driver installation as it copies the files on to your computer.
- Click **Yes** to restart the computer. If your System Settings Change window does not appear, restart your computer: from the Start menu, select **Shut Down > Restart > OK**.

After your PC Port and PC Port driver are successfully installed, repeat Step 3 "Install the Intelligent Gateway Software" on page 12.

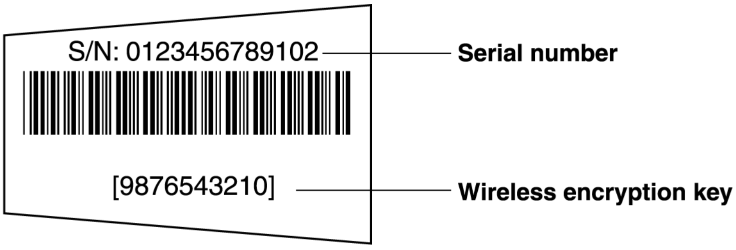
Wireless Connection

Requires a computer with an 802.11b wireless network adapter installed and a 2Wire Wireless PC Card installed in the Intelligent Gateway. Wireless adapters are purchased separately from the Intelligent Gateway.


Telephone socket
Mains power
DSL filter
To telephone (optional)
...in the same room or another room
Computer
(with 802.11b wireless adapter installed)
1
Intelligent Gateway 1800
(with wireless card installed)

1. Install your wireless adapter according to the instructions included with your adapter.

2. Configure your wireless adapter. Your Intelligent Gateway is configured with unique security parameters that must be configured into your wireless adapter. On the bottom of your Intelligent Gateway you will find two important pieces of information required for configuring your adapter: the serial number and the wireless encryption key.



3. Set the network type to **Infrastructure**. Refer to your wireless adapter documentation for instructions on editing the adapter’s network profile. Your wireless adapter should be configured to operate with an access point or residential gateway. This mode of operation is typically enabled by setting network type to Infrastructure.

4. Set the wireless network name (also referred to as SSID). The wireless network name of your Intelligent Gateway is **2WIRE** in all capital letters, followed by the last three digit of the Intelligent Gateway serial number located on the bottom of your Intelligent Gateway. For example, if the last three digits of your Intelligent Gateway serial number are 102, your Intelligent Gateway network name would be 2WIRE102.

The wireless network name is sometimes referred to as the **Network Name**, **SSID**, **ESS ID**, or **Wireless LAN ID**.

5. Enable wireless security. Your Intelligent Gateway automatically configures itself to take advantage of wireless security. Referring to the instructions provided with your wireless adapter, enable wireless security.

Wireless security is sometimes referred to as **WEP** (wired equivalent privacy), **64-bit encryption**, or **40-bit encryption**.

6. Enter the encryption key. Once you have enabled security on your wireless adapter, you need to enter the unique security key for your Intelligent Gateway. To do this, set the network encryption type to **hexadecimal**, and enter your 10-digit wireless encryption key found on the bottom of your Intelligent Gateway. For Macintosh computers, the encryption key must be prefixed with a “$.”

Note: *To maximize your wireless network security, it is recommended that you change the WEP key on a regular basis and/or enable 128-bit encryption (if your PC card or adapter supports 128-bit encryption). Doing so will make it harder for hackers to access your wireless network.*

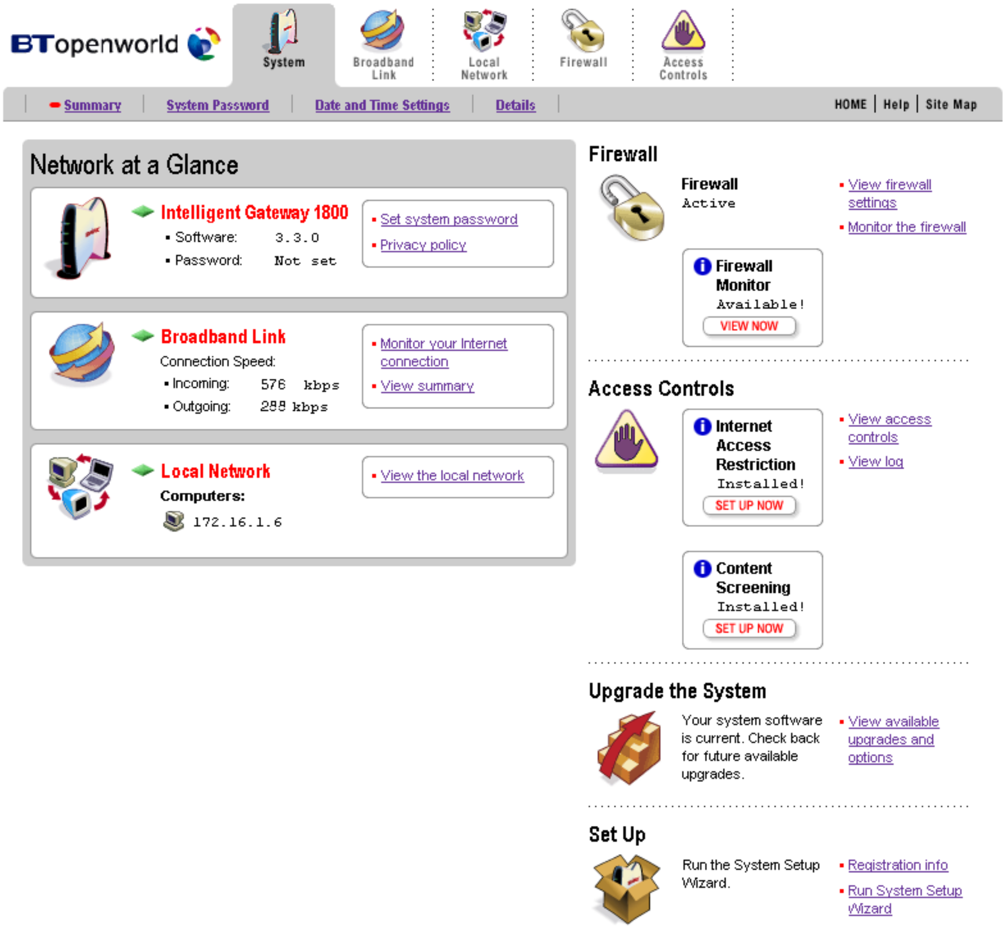
Note: *For optimal performance, it is recommended that you locate computers in your wireless network no farther apart than 50 feet. The 50-foot limitation for wireless networks is based on the assumption that most users are located in a many-walled or multi-story building. If you are using a wireless network in an outdoor space, your range may be greater.*

Repeat Step 3 “Install the Intelligent Gateway Software” on page 12.

Using the Intelligent Gateway Network

The Intelligent Gateway user interface allows you to check the status of your network, assign permissions to other users on the network, and access links to the most commonly used features of your Intelligent Gateway.

After you have connected your computers to your network and installed the Intelligent Gateway software, enter http://home in the address bar of your browser. The Intelligent Gateway user interface opens.



Network at a Glance

Intelligent Gateway 1800
- Software: 3.3.0
- Password: Not set

- Set system password
- Privacy policy

Broadband Link

Connection Speed:
- Incoming: 576 kbps
- Outgoing: 288 kbps

- Monitor your Internet connection
- View summary

Local Network

Computers:

172.16.1.6

- View the local network

Firewall

Firewall Active

- View firewall settings
- Monitor the firewall

Firewall Monitor Available! VIEW NOW

Access Controls

Internet Access Restriction Installed! SET UP NOW

- View access controls
- View log

Content Screening Installed! SET UP NOW

Upgrade the System

Your system software is current. Check back for future available upgrades.

- View available upgrades and options

Set Up

Run the System Setup Wizard.

- Registration info
- Run System Setup Wizard

System

The System pages provide you with general system information and operational status.

- The Summary page is your system home page. You can access this page by clicking the **HOME** icon from any system page. The Summary page provides summary information and links to the most commonly used features of your system.
- The System Password page allows you to password protect local access to your system settings, preventing users on your local network from changing your system configuration. If a system password is set, only local users who know the system password can change system settings (for example, broadband connection parameters and firewall settings).
- The Date and Time Settings page displays your system date and time settings, and allows you to edit these settings as needed.
- The Details page displays information about your system's hardware and software configuration, and provides links to detailed system level access and information.

Viewing your summary

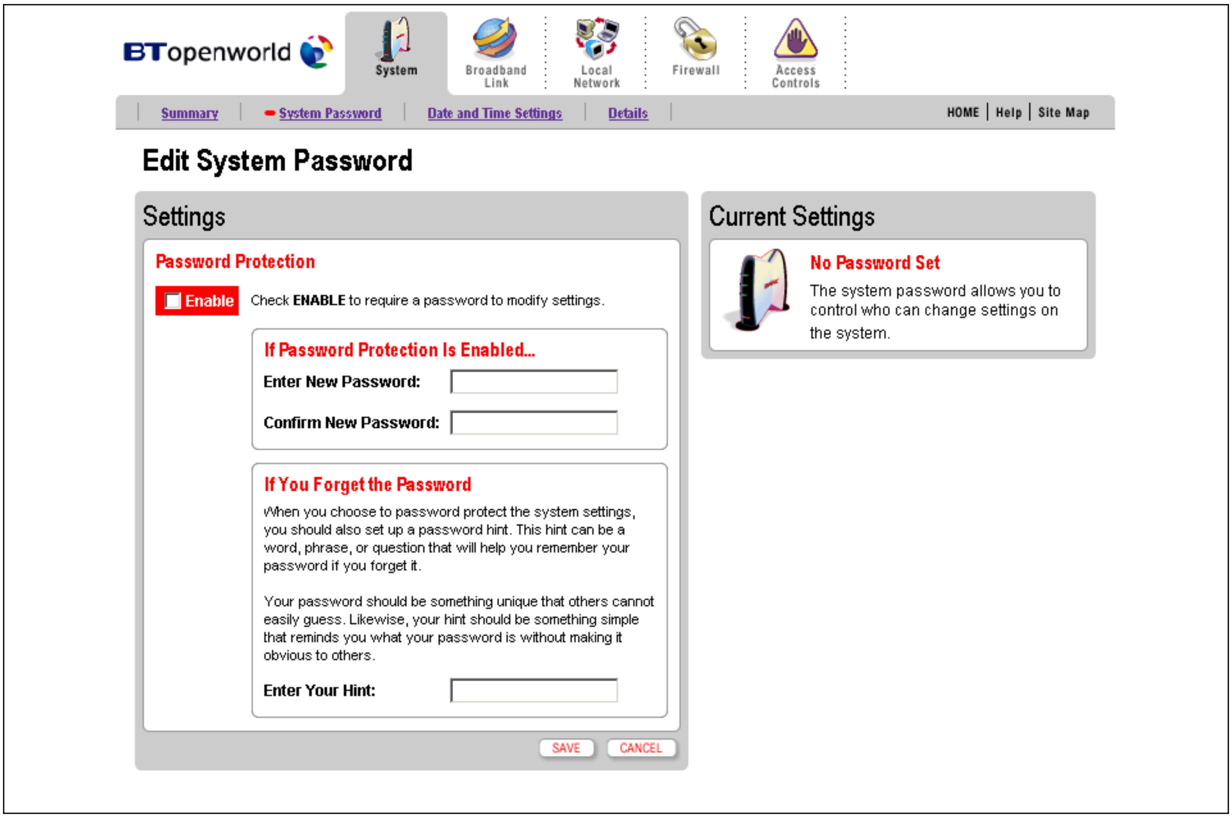
The Summary page provides general information and links to your system's most commonly used features. This page consists of the Network at a Glance panel to the left, and a list of subsections to the right. These subsections will vary depending on the options and services installed on your system.

The Network at a Glance panel provides a quick summary of broadband and local network connectivity information, and the system's overall status.

- System displays your Intelligent Gateway's Power light status, the model name, the version of system software that you are using, and the status of your system password.
- Broadband Link displays a summary of your Broadband Link status.
- Local Network displays your system's Local Network light status and a list of the devices currently connected to your local network.

Editing your system password

If a system password has been set, the system will prompt you to enter the password when accessing any page where you can change settings. If a password has not been set, a reminder notice is displayed in some of the more sensitive topic areas. Setting a system password will ensure that only you are permitted to make changes to your system settings.



Edit System Password

Settings

Password Protection

☐ Enable Check **ENABLE** to require a password to modify settings.

If Password Protection Is Enabled...

Enter New Password:

Confirm New Password:

If You Forget the Password

When you choose to password protect the system settings, you should also set up a password hint. This hint can be a word, phrase, or question that will help you remember your password if you forget it.

Your password should be something unique that others cannot easily guess. Likewise, your hint should be something simple that reminds you what your password is without making it obvious to others.

Enter Your Hint:

Current Settings

No Password Set

The system password allows you to control who can change settings on the system.

Setting a password

To set your Intelligent Gateway system password:

1. Check the **Enable** checkbox.
2. In the Enter New Password field, enter your password.
3. In the Confirm New Password field, re-enter your password.
4. (Optional) In the Enter Your Hint field, enter a hint.
5. Click the **SAVE** button.

To disable password protection, deselect the **Enable** checkbox and click **SAVE**.

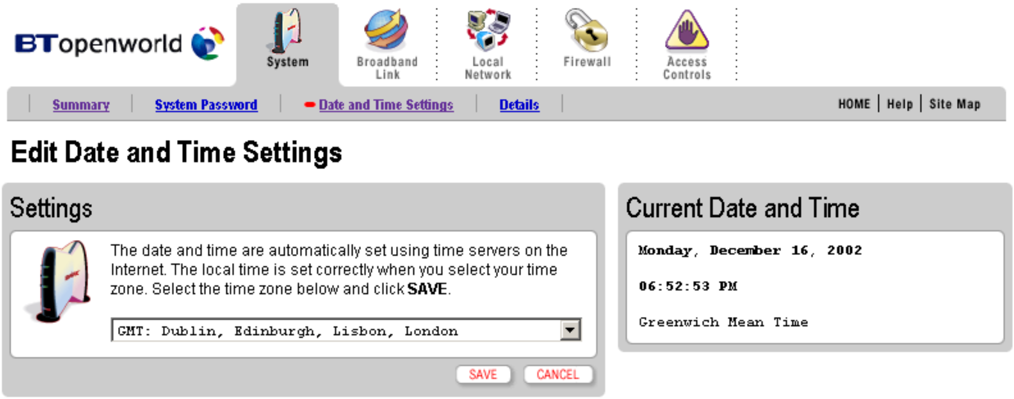
Changing a password

To change your Intelligent Gateway system password:

1. In the Enter Current Password field, enter your current system password.
2. In the Enter New Password field, enter your new password.
3. In the Confirm New Password field, re-enter your new password.
4. (Optional) In the Enter Your Hint field, enter a hint.
5. Click the **SAVE** button.

Editing your date and time settings

The Intelligent Gateway automatically sets the time using time servers on the Internet, or from the PC if no Internet connection is available. It retrieves date/time information in Greenwich Mean Time (GMT). Your local time is set using the Time Zone setting you configured when you set up your system.



Edit Date and Time Settings

Settings

The date and time are automatically set using time servers on the Internet. The local time is set correctly when you select your time zone. Select the time zone below and click **SAVE**.

GMT: Dublin, Edinburgh, Lisbon, London

Current Date and Time

Monday, December 16, 2002

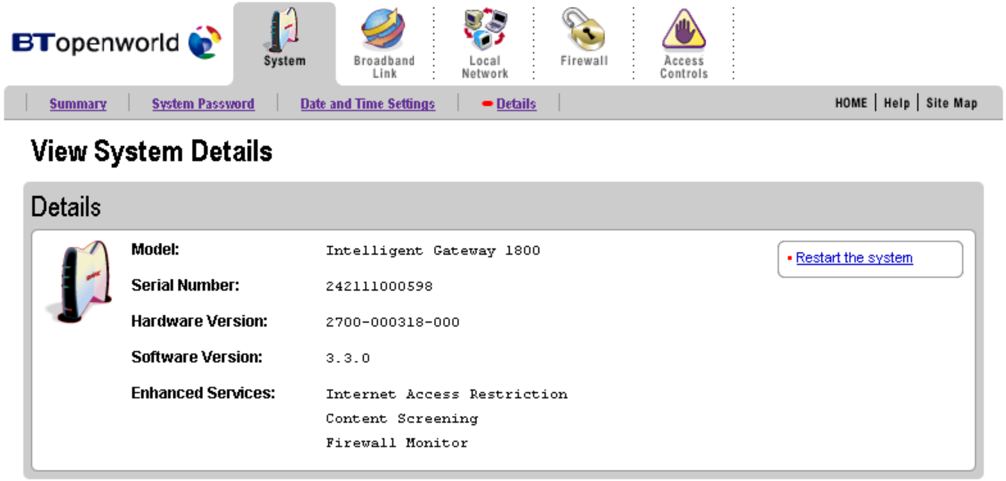
06:52:53 PM

Greenwich Mean Time

If your wish to change your time zone:

1. In the Settings panel, select a time zone from the pull-down menu.
2. Click the **SAVE** button.

Viewing your system details



View System Details

Details

Model:	Intelligent Gateway 1800
Serial Number:	242111000598
Hardware Version:	2700-000318-000
Software Version:	3.3.0
Enhanced Services:	Internet Access Restriction Content Screening Firewall Monitor

The System Details page provides the following information about your system:

- Model. The Intelligent Gateway model number (for example, 1800).
- Serial Number. The Intelligent Gateway serial number.
- Hardware Version. The Intelligent Gateway hardware version.
- Software Version. The software version the Intelligent Gateway is currently running.
- Enhanced Services. The enhanced services currently installed on your system.

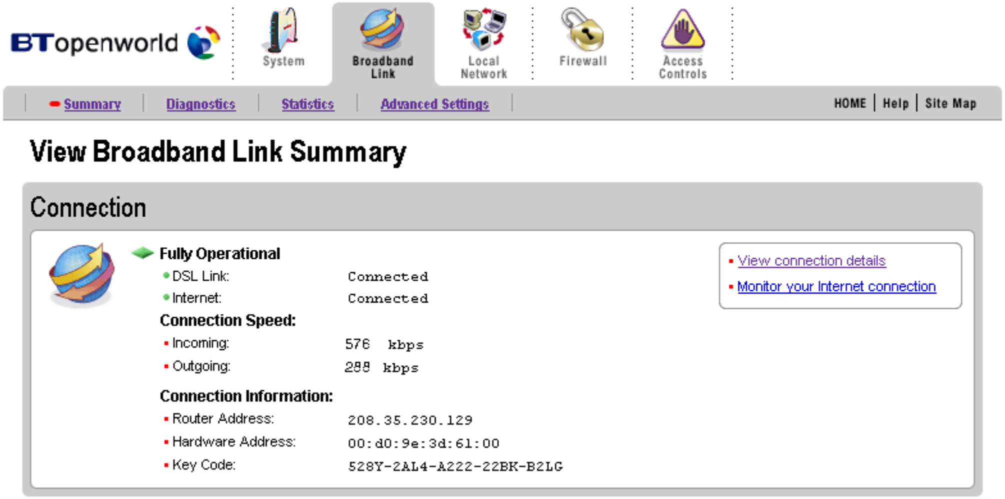
To restart your system, click the **Restart the system** link. Your local network connections and your broadband connectivity will be briefly disrupted until your system restarts and broadband connectivity is re-established.

Broadband Link

The Broadband Link pages show general information about your broadband link connection and system configuration, and allows advanced users to manually configure their DSL and Internet connection settings.

Viewing your Broadband Link summary

The Broadband Link Summary page provides general information about the current status and speed of your broadband link connection, and your system configuration.



View Broadband Link Summary

Connection

Fully Operational

- DSL Link: Connected
- Internet: Connected

Connection Speed:

- Incoming: 576 kbps
- Outgoing: 288 kbps

Connection Information:

- Router Address: 208.35.230.129
- Hardware Address: 00:d0:9e:3d:61:00
- Key Code: 528Y-2AL4-A222-22BK-B2LG

Checking your connection details

You can check the current status of your Intelligent Gateway's broadband connection by using the **BROADBAND LINK** indicator light on the front of your Intelligent Gateway or, if your computer is connected to the network, you can view the status in the Connection panel.

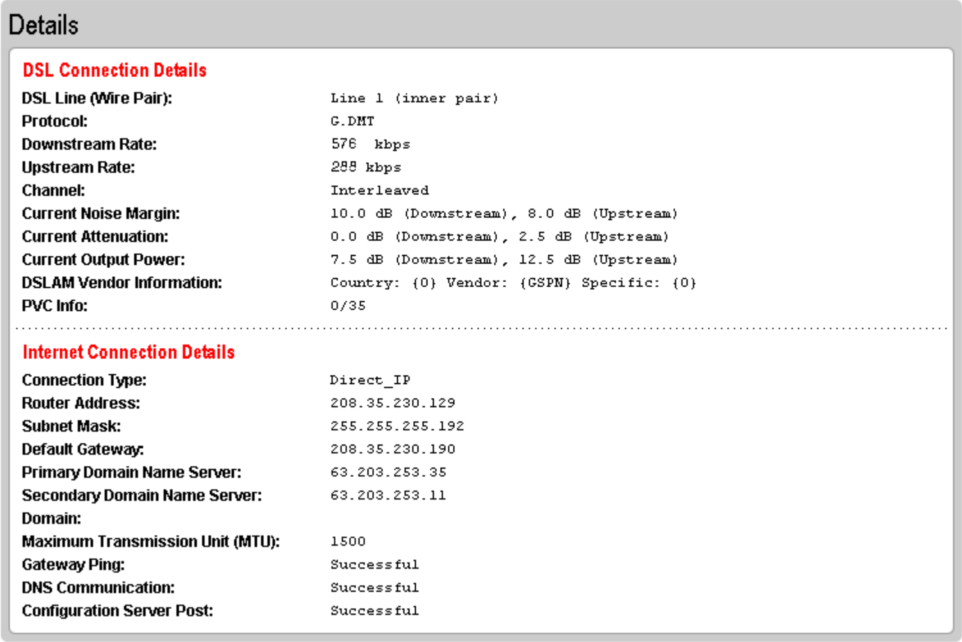
Viewing connection information

The Connection Information box shows basic system configuration information.

- Router Address. The broadband IP address assigned by your service provider to your system so that it can communicate on the Internet. The address is either Static (permanently assigned and manually entered) or Dynamic (automatically assigned and configured), depending on the service type to which you have subscribed.
- Hardware Address. The hardware address is also known as the MAC address or physical address. When your system is connected to the broadband network, an association is made between its unique hardware address and its Internet address before it can communicate to the Internet.
- Key Code. The activation code that tells your system how to connect to your service provider. The key code is used during the system installation process to customize the setup screens and settings for your broadband provider.

Viewing connection details

Click the **View connection details** link to view technical information about your broadband connection. This information is used by technical support representatives to aid them in troubleshooting a problem with your broadband connection.



Details

DSL Connection Details

DSL Line (Wire Pair):	Line 1 (inner pair)
Protocol:	G.DMT
Downstream Rate:	576 kbps
Upstream Rate:	288 kbps
Channel:	Interleaved
Current Noise Margin:	10.0 dB (Downstream), 8.0 dB (Upstream)
Current Attenuation:	0.0 dB (Downstream), 2.5 dB (Upstream)
Current Output Power:	7.5 dB (Downstream), 12.5 dB (Upstream)
DSLAM Vendor Information:	Country: {0} Vendor: {GSPN} Specific: {0}
PVC Info:	0/35

Internet Connection Details

Connection Type:	Direct_IP
Router Address:	208.35.230.129
Subnet Mask:	255.255.255.192
Default Gateway:	208.35.230.190
Primary Domain Name Server:	63.203.253.35
Secondary Domain Name Server:	63.203.253.11
Domain:	
Maximum Transmission Unit (MTU):	1500
Gateway Ping:	Successful
DNS Communication:	Successful
Configuration Server Post:	Successful

DSL connection details

The DSL Connection Details panel shows the following information:

Field	Description
DSL Line (Wire pair)	The DSL signal is primarily transmitted on Line 1 (inner pair). During installation, the system automatically detects on which line the DSL signal is being transmitted.
Protocol	Displays which DSL protocol is being used to communicate between your system and your service provider.
Downstream Rate	The speed at which data comes over your broadband connection from the Internet to your network. Data transfer speeds are measured in kilobits per second (kbps).
Upstream Rate	The speed at which data goes over your broadband connection from your network to the Internet. Data transfer speeds are measured in kilobits per second (kbps).
Channel	This setting is determined by BT Openworld's DSLAM equipment.
Current Noise Margin	Indicates how much the noise on the DSL line can increase before it begins to affect the DSL signal. As the noise on the DSL line increases, the margin will approach zero. If the noise exceeds the current noise margin, the DSL signal will be lost. The level is measured in decibels (dBs).
Current Attenuation	Represents the decrease in signal strength between origination of the DSL (Telephone Exchange) and your system. Customers who live close to their Telephone Exchange usually will have less signal loss and a low current attenuation. The level is measured in decibels (dBs)

Field	Description
Current Output Power	The current DSL transmit power of your system. The level is measured in decibels (dBs).
DSLAM Vendor Information	A DSLAM is the piece of equipment located in the Telephone Exchange that provides the DSL signal to your DSL line. The Vendor Information identifies information about the configuration of this equipment.
PVC Info	Displays the pair of numbers that uniquely identifies the ATM virtual circuit between the system and the provider of your DSL service.

Internet connection details

The Internet Connection Details panel shows the following information:

Field	Description
Connection Type	Identifies the method by which the system connects to the ISP: PPPoE, PPPoA, or Direct.
Internet Address	The number that is assigned to a computer so that it can communicate on a network and on the Internet. This address is assigned to you by your ISP for all communication on the Internet, and can either be Static (permanently assigned and manually entered) or Dynamic (automatically assigned and configured). Typically your ISP automatically assigns and configures an Internet address (dynamic) when your system connects to the Internet. Businesses or power users may use a static address enabling them to run advanced services such as Internet servers and video conferencing. If you receive your Internet Address settings automatically, the subnet mask has been set for you. If you manually set your Internet Address (static IP), this is the information that was provided to you by BT Openworld and entered by you during system installation.
Subnet Mask	The subnet mask is part of the Internet Address settings and is used in conjunction with your Internet Address. If you receive your Internet Address settings automatically, the subnet mask has been set for you. If you manually set your Internet Address (static IP), this is the information that was provided to you by BT Openworld and entered by you during system installation.
Default Gateway	The Default Gateway is part of the Internet Address settings. The default gateway is a device your system communicates with directly to give you access to the Internet. If you receive your Internet Address settings automatically, the subnet mask has been set for you. If you manually set your Internet Address (static IP), this is the information that was provided to you by BT Openworld and entered by you during system installation.
Primary Domain Name Server	The Primary Domain Name Server (DNS) is part of the Internet Address settings. A domain name is a meaningful, easy-to-remember “handle” for an Internet address. The DNS allows Internet users to specify a name (domain name) to reach a Web page (for example, www.domainname.com) instead of its Internet address (for example, 111.222.111.222). When you enter the name of a Web location (URL), the DNS looks up the name and resolves it to the Web page’s Internet address. If you receive your Internet Address settings automatically, the subnet mask has been set for you. If you manually set your Internet Address (static IP), this is the information that was provided to you by BT Openworld and entered by you during system installation.

Field	Description
Secondary Domain Name Server	The Secondary Domain Name Server is used as a backup if the Primary server fails to respond. If you receive your Internet Address settings automatically, the subnet mask has been set for you. If you manually set your Internet Address (static IP) this is the information that was provided to you by BT Openworld and entered by you during system installation. This parameter may not be necessary and may be left blank.
Domain	The name that associates your system with your ISP on the broadband link. This parameter may not be necessary and may be left blank. If you receive your Internet Address settings automatically, the subnet mask has been set for you. If you manually set your Internet Address (static IP), this is the information that was provided to you by BT Openworld and entered by you during system installation.
Maximum Transmission Unit (MTU)	Shows the maximum size allowed on packets that are sent to and from your network to BT Openworld.
Gateway Ping	The Intelligent Gateway periodically checks the connection between your system and BT Openworld's Default Gateway. This field informs you that the check has been performed and whether or not it was successful.
DNS Communication	The Intelligent Gateway periodically checks the connection between your system and BT Openworld’s domain name server(s) to make sure DNS is available. This field informs you that the check has been performed and whether or not it was successful.
Configuration Server Post	The Intelligent Gateway periodically checks the connection between your system and the Component Management System. This field informs you that the check has been performed and whether or not it was successful.

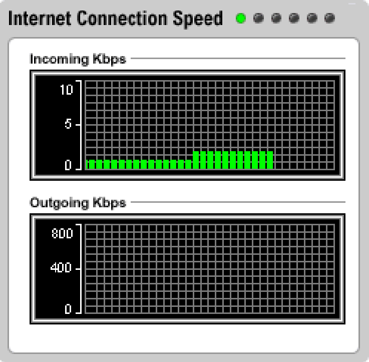
Checking your connection speed

The Connection Speed box shows the incoming and outgoing data rates of your DSL connection.

- Incoming. The speed of data flowing from the Internet to your network. Data transfer speeds are measured in kilobits per second (Kbps).
- Outgoing. The speed of data flowing from your network to the Internet. Data transfer speeds are measured in kilobytes per second (Kbps).

Monitoring your Internet connection

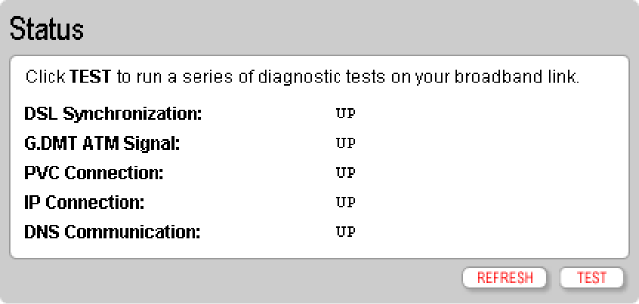
Click the **Monitor Internet connection** link to launch the Speed Meter.The Speed Meter measures the actual rate at which data is coming into (Incoming Kbps) and going out of (Outgoing Kbps) your system. It measures real-time data throughput in Kilobits per second and displays in one-second intervals. This data rate can differ from the reported speed of your broadband connection due to many factors, including traffic to the Web site or the speed of the Web servers at the site you are visiting.



Note: *The Speed Meter requires that your browser support Java 2.*

Using Broadband Link diagnostics

The Broadband Link Diagnostics page displays an itemized list of your broadband connection's current status (DSL Synchronization, G.DMT ATM Signal, PVC and IP Connection, and DNS Communication). To update the broadband link detailed status, click **REFRESH**. To run a full test of your broadband link, click **TEST**. The test will take several minutes, during which time you will not be able to access the Internet.

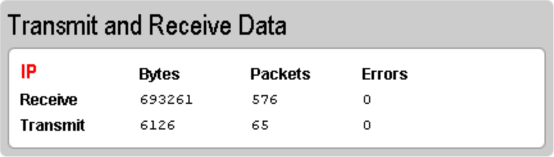


Click **TEST** to run a series of diagnostic tests on your broadband link.

DSL Synchronization:	UP
G.DMT ATM Signal:	UP
PVC Connection:	UP
IP Connection:	UP
DNS Communication:	UP

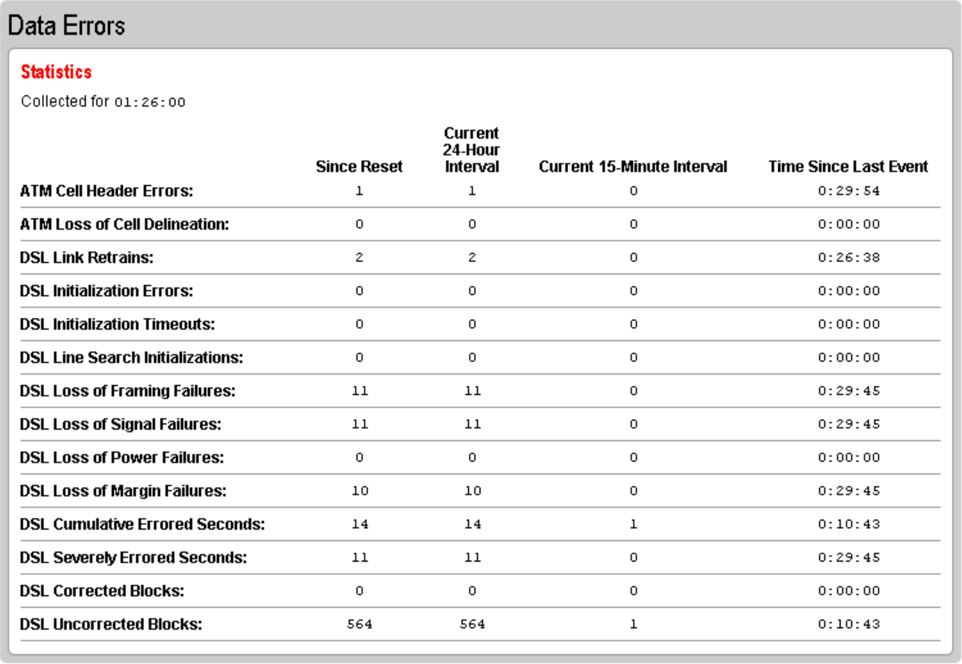
Viewing Broadband Link statistics

The Intelligent Gateway keeps a running count of DSL activity in and out of your Internet connection since the last reset, and tracks errors that occurred on your DSL connection. The Transmit and Receive Data panel shows the total number of data bytes and IP packets either transmitted or received, and the total number of IP errors transmitted and received since the last reset. The Data Errors panel shows accumulated data errors from when your system is started until a reset. Accumulated errors do not necessarily indicate a problem with your broadband service or your system.



Transmit and Receive Data

IP	Bytes	Packets	Errors
Receive	693261	576	0
Transmit	6126	65	0



Data Errors

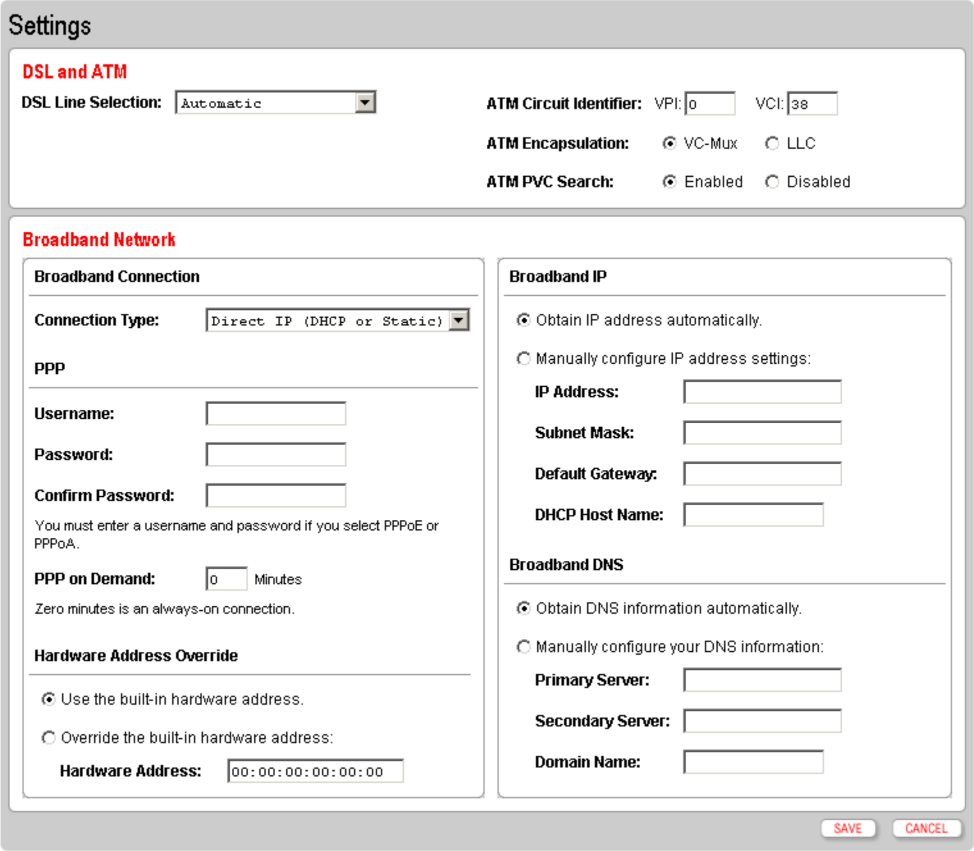
Statistics

Collected for 01:26:00

	Since Reset	Current 24-Hour Interval	Current 15-Minute Interval	Time Since Last Event
ATM Cell Header Errors:	1	1	0	0:29:54
ATM Loss of Cell Delineation:	0	0	0	0:00:00
DSL Link Retrains:	2	2	0	0:26:38
DSL Initialization Errors:	0	0	0	0:00:00
DSL Initialization Timeouts:	0	0	0	0:00:00
DSL Line Search Initializations:	0	0	0	0:00:00
DSL Loss of Framing Failures:	11	11	0	0:29:45
DSL Loss of Signal Failures:	11	11	0	0:29:45
DSL Loss of Power Failures:	0	0	0	0:00:00
DSL Loss of Margin Failures:	10	10	0	0:29:45
DSL Cumulative Errored Seconds:	14	14	1	0:10:43
DSL Severely Errored Seconds:	11	11	0	0:29:45
DSL Corrected Blocks:	0	0	0	0:00:00
DSL Uncorrected Blocks:	564	564	1	0:10:43

Modifying Broadband Link settings

The Advanced Settings page allows advanced users to manually configure their DSL and Internet connection settings. You should only modify the connection settings if you are very familiar with DSL and networking technology.



Settings

DSL and ATM

DSL Line Selection: Automatic

ATM Circuit Identifier: VPI: 0 VCI: 38

ATM Encapsulation: ● VC-Mux ○ LLC

ATM PVC Search: ● Enabled ○ Disabled

Broadband Network

Broadband Connection

Connection Type: Direct IP (DHCP or Static)

PPP

Username:

Password:

Confirm Password:

You must enter a username and password if you select PPPoE or PPPoA.

PPP on Demand: 0 Minutes

Zero minutes is an always-on connection.

Hardware Address Override

● Use the built-in hardware address.

○ Override the built-in hardware address:

Hardware Address: 00:00:00:00:00:00

Broadband IP

● Obtain IP address automatically.

○ Manually configure IP address settings:

IP Address:

Subnet Mask:

Default Gateway:

DHCP Host Name:

Broadband DNS

● Obtain DNS information automatically.

○ Manually configure your DNS information:

Primary Server:

Secondary Server:

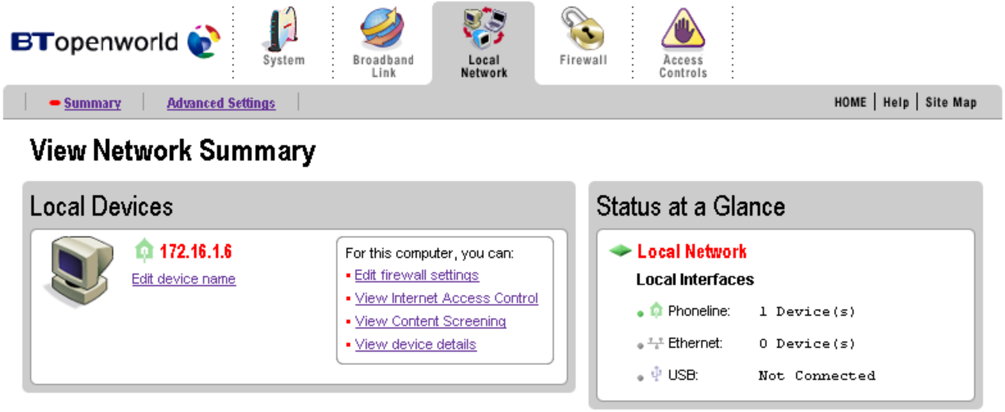
Domain Name:

Local Network

The Local Network pages show summary information about the devices in your network, and allow you to configure the devices.

Viewing Local Network summary information

The Local Devices panel displays the name of the device, how it is connected, any special configuration information, and gives you links to other system features that you can set up for the device.



View Network Summary

Local Devices

172.16.1.6
Edit device name

For this computer, you can:
- Edit firewall settings
- View Internet Access Control
- View Content Screening
- View device details

Status at a Glance

Local Network

Local Interfaces

Phoneline:	1 Device(s)
Ethernet:	0 Device(s)
USB:	Not Connected

The following information may display:

- Device. The device symbol is represented with a computer icon. If the “show inactive devices” option on the advanced settings page is enabled, and the device becomes inactive because it is powered off or removed from your network, this symbol will display as Inactive.
- Network Type. A symbol representing the type of network connection this device has to your system (Ethernet, USB, HomePNA, or Wireless).
- Name. The name that was defined for your computer during the System Setup or when your computer was set up. However, there are two instances where the device name will not appear. If a computer has been manually configured with a static IP address, the IP address is displayed instead of the computer’s name. Similarly, if a device does not have a name but still obtains an Internet address from the system, it will display as Unknown.
- Change Name. This link appears only for devices that have been manually assigned a static IP address, or for devices that do not report a device name to the system. You can change the name of the device in the system user interface.
- Hosting List. A list of the applications that are allowed to pass through the firewall. To host an application for use from the Internet, you must install the application on a computer and configure the firewall to allow information from the Internet to pass through to the computer.

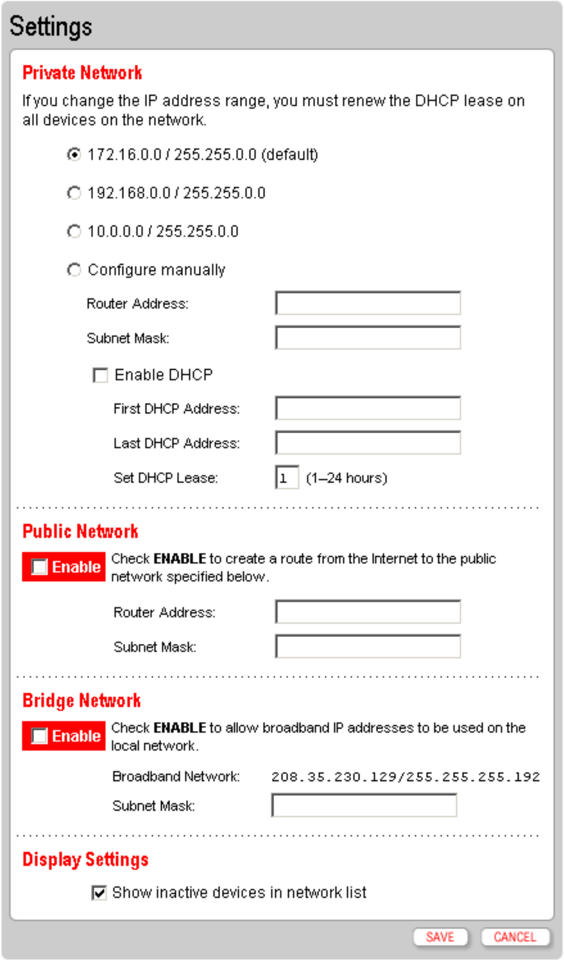
The box to the right of the Local Devices panel contains links to other system features that can be viewed or configured for this device. Certain links may not apply for each device. The following lists the possible links:

- Access shared files. Click this link to access the shared files available from this computer. This feature only works with Microsoft Windows computers that have shared files and file sharing configured.
- Edit firewall settings. Click this link to access the Edit Firewall Settings page, which allows you to edit the firewall pass-through settings for that specific computer. You may need to change the pass-through settings for this computer if, for example, you wanted to play an Internet game on that computer.
- View Internet Access Control. Click this link to access the Internet Access Restriction Settings page, which displays the Internet Access Restrictions Schedule currently set for this computer.
- View Content Screening. Click this link to access the Content Screenings Settings page, which displays the Content Screening settings for this computer.
- View device details. This link displays the technical networking details about the device.

The Status at a Glance panel shows you the current status of your local network, a list of the types of network connections, and how many devices are connected via each network type.

Editing advanced Local Network settings

The Advanced Settings page allows advanced users to change their default local network settings. These settings should only be modified if you are very familiar with computer networking technology.



Settings

Private Network

If you change the IP address range, you must renew the DHCP lease on all devices on the network.

● 172.16.0.0 / 255.255.0.0 (default)

○ 192.168.0.0 / 255.255.0.0

○ 10.0.0.0 / 255.255.0.0

○ Configure manually

Router Address:

Subnet Mask:

□ Enable DHCP

First DHCP Address:

Last DHCP Address:

Set DHCP Lease: 1 (1–24 hours)

Public Network

□ Enable Check **ENABLE** to create a route from the Internet to the public network specified below.

Router Address:

Subnet Mask:

Bridge Network

□ Enable Check **ENABLE** to allow broadband IP addresses to be used on the local network.

Broadband Network: 208.35.230.129/255.255.255.192

Subnet Mask:

Display Settings

☑ Show inactive devices in network list

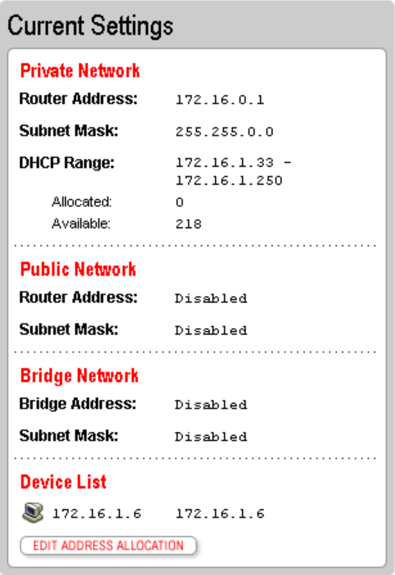
- **Private Network.** Sets the IP address range used by the local network. You can choose from three standard configuration options or configure the network settings manually. If you choose manual configuration, you must understand IP internetworking thoroughly. An incorrect configuration can cause unpredictable results on your local network.

Note: *If you change the local network IP address range, you must renew the DHCP lease on all devices on your local network and manually reconfigure all devices configured with static IP addresses.*

- **Public Network.** Creates a local network that has broadband network-accessible IP addresses by creating a route from the Internet to the public network specified. The public network operates without the use of Network Address Translation (NAT). This feature is typically used in conjunction with broadband service that provides a range of available IP addresses. Once enabled, the public IP addresses can be assigned to local computers.
- **Bridge Network.** Creates a local network that has broadband-accessible IP addresses. Bridge Network is a public network in which the local network is an extension of the broadband network and does not require any special routing. Computers that are assigned Bridge Network IP addresses operate without the use of Network Address Translation (NAT). This feature is typically used in conjunction with broadband service that provides a range of IP addresses. Once enabled, the bridge network IP addresses can be assigned to local computers.
- **Display Settings.** If the **Show Inactive Devices** checkbox is checked, devices that are no longer on the local network will display in the Local Network Local Devices list as an inactive device. If this box is not checked, inactive devices will not be displayed in the device list.

Changing address allocation

The Current Settings panel displays the computers currently on the local network and the IP address associated with each computer. It also indicates whether a given computer is receiving its IP address via DHCP or has been manually entered into the computer (static).



Current Settings

Private Network

Router Address: 172.16.0.1

Subnet Mask: 255.255.0.0

DHCP Range: 172.16.1.33 - 172.16.1.250

Allocated: 0

Available: 218

Public Network

Router Address: Disabled

Subnet Mask: Disabled

Bridge Network

Bridge Address: Disabled

Subnet Mask: Disabled

Device List

172.16.1.6 172.16.1.6

If you have enabled either the Public Network or Bridge Network feature, you can choose to have your broadband accessible (non-NAT) IP addresses assigned automatically via DHCP to computers on the local network. To do so:

1. From the Current Settings panel, click the **Edit Address Allocation** button.
2. From the IP Address pull-down menu, select an address from any of the available networks.
3. Click the **SAVE** button.

Computers that are assigned non-routable (private network) addresses will use Network Address Translation (NAT) to access the Internet. Choosing a “DHCP Fixed” entry instructs the Intelligent Gateway to always provide the same address from the DHCP pool to the specified computer.

Note: *Computers on either the Public Network or Bridge Network are still behind the firewall. To allow inbound traffic to these computers, you must modify the firewall settings specified for that computer.*

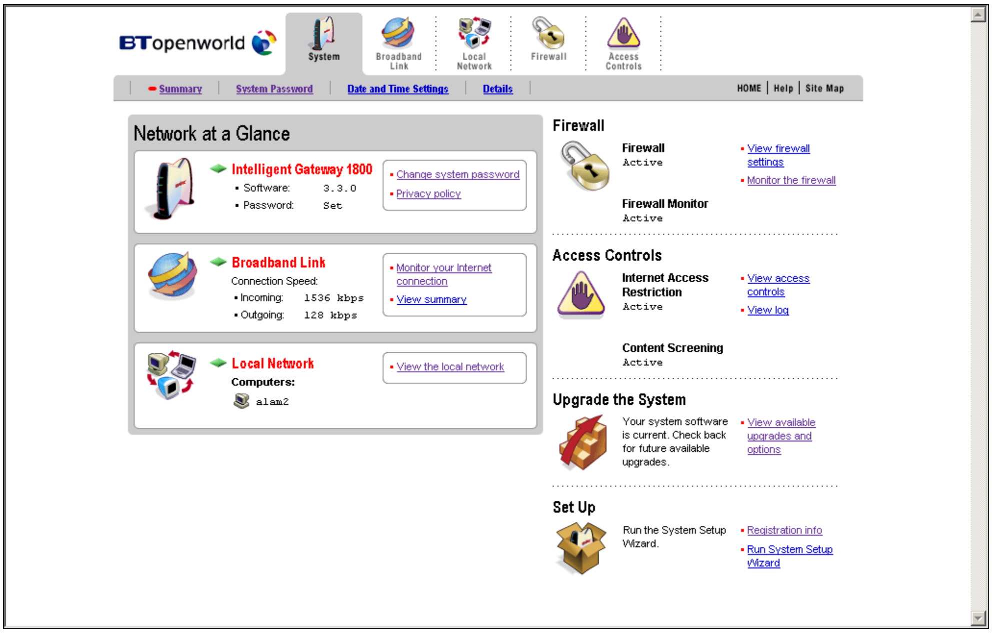
Connecting to a corporate LAN via VPN

A Virtual Private Network (VPN) is a secure connection that allows remote users and telecommuters to connect to the corporate LAN using the public Internet.

The Intelligent Gateway supports VPN clients such as Nortel, Cisco, Checkpoint, and Microsoft (IPSec and PPTP). Ensure that your company is using VPN software that is compatible with the Intelligent Gateway.

If you cannot transfer data while using your VPN, check with your corporate IT manager and ensure that your corporate network is not using the 172.xxx.xxx.xxx IP scheme (the Intelligent Gateway default). You cannot connect to a VPN server that uses the same IP scheme as your Intelligent Gateway. If your company is using a 172.x.x.x IP scheme, change the Intelligent Gateway local network IP configuration range by following these steps.

1. Open the Intelligent Gateway home page.



Network at a Glance

Intelligent Gateway 1800
- Software: 3.3.0
- Password: Set

- Change system password
- Privacy policy

Broadband Link
Connection Speed:
- Incoming: 1536 kbps
- Outgoing: 128 kbps

- Monitor your Internet connection
- View summary

Local Network
Computers:
alam2

- View the local network

Firewall

Firewall
Active

Firewall Monitor
Active

- View firewall settings
- Monitor the firewall

Access Controls

Internet Access Restriction
Active

Content Screening
Active

- View access controls
- View log

Upgrade the System

Your system software is current. Check back for future available upgrades.

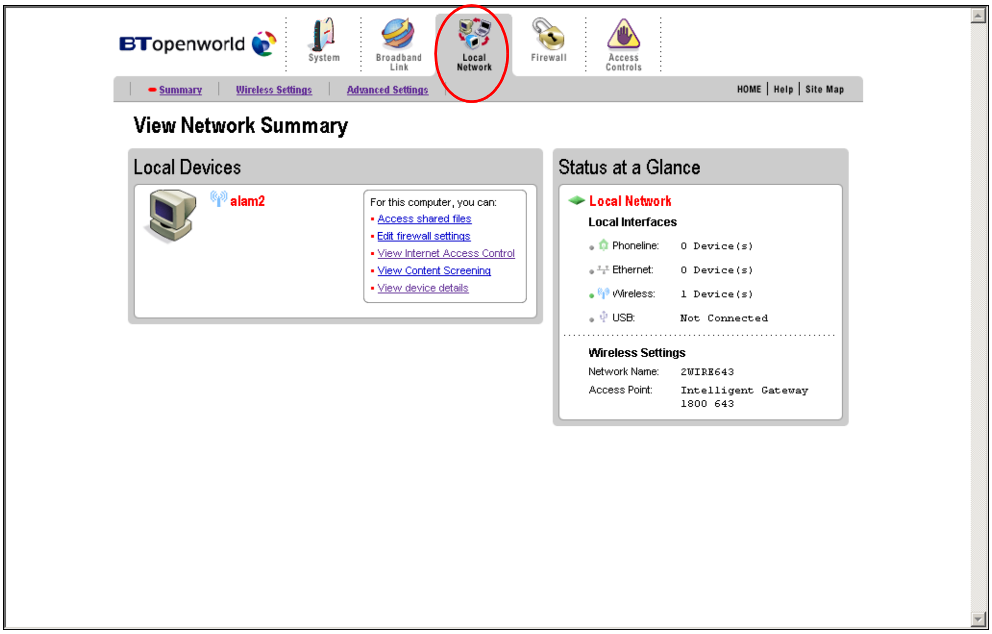
- View available upgrades and options

Set Up

Run the System Setup Wizard.

- Registration info
- Run System Setup Wizard

2. Click the Local Network tab.



View Network Summary

Local Devices

alam2

For this computer, you can:
- Access shared files
- Edit firewall settings
- View Internet Access Control
- View Content Screening
- View device details

Status at a Glance

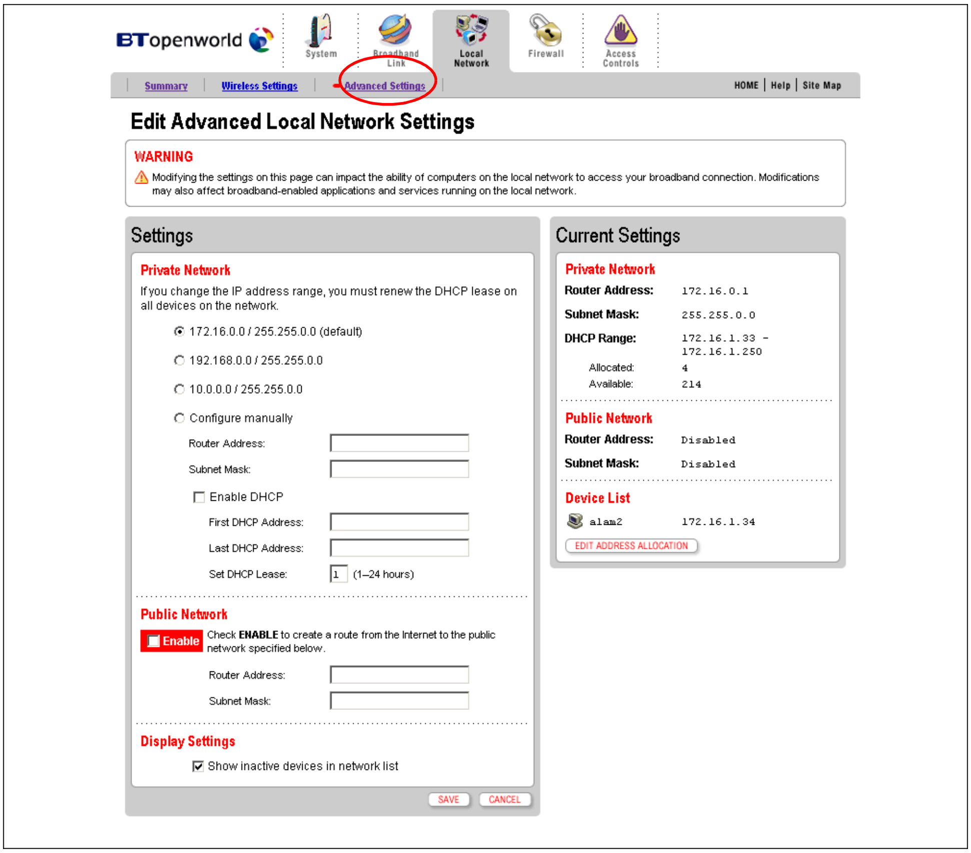
Local Network
Local Interfaces

Phoneline:	0 Device(s)
Ethernet:	0 Device(s)
Wireless:	1 Device(s)
USB:	Not Connected

Wireless Settings

Network Name:	2WIRE643
Access Point:	Intelligent Gateway 1800 643

3. Click Advanced Settings.



Edit Advanced Local Network Settings

WARNING

⚠ Modifying the settings on this page can impact the ability of computers on the local network to access your broadband connection. Modifications may also affect broadband-enabled applications and services running on the local network.

Settings

Private Network

If you change the IP address range, you must renew the DHCP lease on all devices on the network.

● 172.16.0.0 / 255.255.0.0 (default)

○ 192.168.0.0 / 255.255.0.0

○ 10.0.0.0 / 255.255.0.0

○ Configure manually

Router Address:

Subnet Mask:

□ Enable DHCP

First DHCP Address:

Last DHCP Address:

Set DHCP Lease: 1 (1–24 hours)

Public Network

□ Enable Check **ENABLE** to create a route from the Internet to the public network specified below.

Router Address:

Subnet Mask:

Display Settings

☑ Show inactive devices in network list

SAVE CANCEL

Current Settings

Private Network

Router Address:	172.16.0.1
Subnet Mask:	255.255.0.0
DHCP Range:	172.16.1.33 - 172.16.1.250
Allocated:	4
Available:	214

Public Network

Router Address:	Disabled
Subnet Mask:	Disabled

Device List

alam2 172.16.1.34

EDIT ADDRESS ALLOCATION

4. In the Settings pane, change the LAN IP range to either 10.xxx.xxx.xxx or 192.xxx.xxx.xxx by clicking the corresponding radio button.

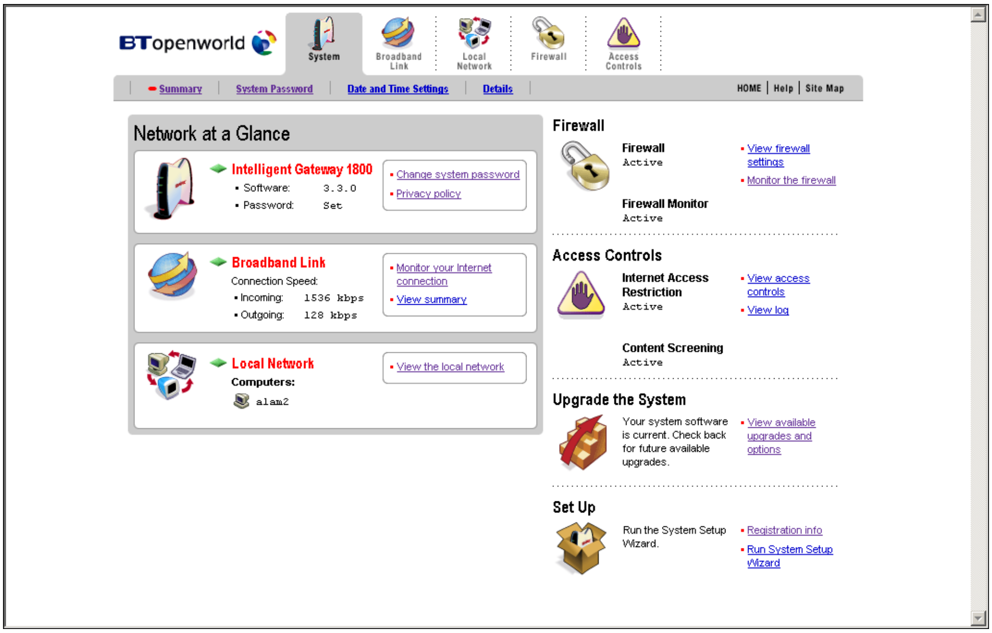
5. Click the **SAVE** button.

You must release and renew the IP address on your computer for the change to take effect.

Maintaining/restoring the VPN connection

If your VPN client regularly loses its connection, you can increase the time before the computer requires a new IP address by following these steps.

1. Open the Intelligent Gateway home page.



Network at a Glance

Intelligent Gateway 1800
- Software: 3.3.0
- Password: Set

- Change system password
- Privacy policy

Broadband Link
Connection Speed:
- Incoming: 1536 kbps
- Outgoing: 128 kbps

- Monitor your Internet connection
- View summary

Local Network
Computers:
alam2

- View the local network

Firewall

Firewall
Active

Firewall Monitor
Active

- View firewall settings
- Monitor the firewall

Access Controls

Internet Access Restriction
Active

Content Screening
Active

- View access controls
- View log

Upgrade the System

Your system software is current. Check back for future available upgrades.

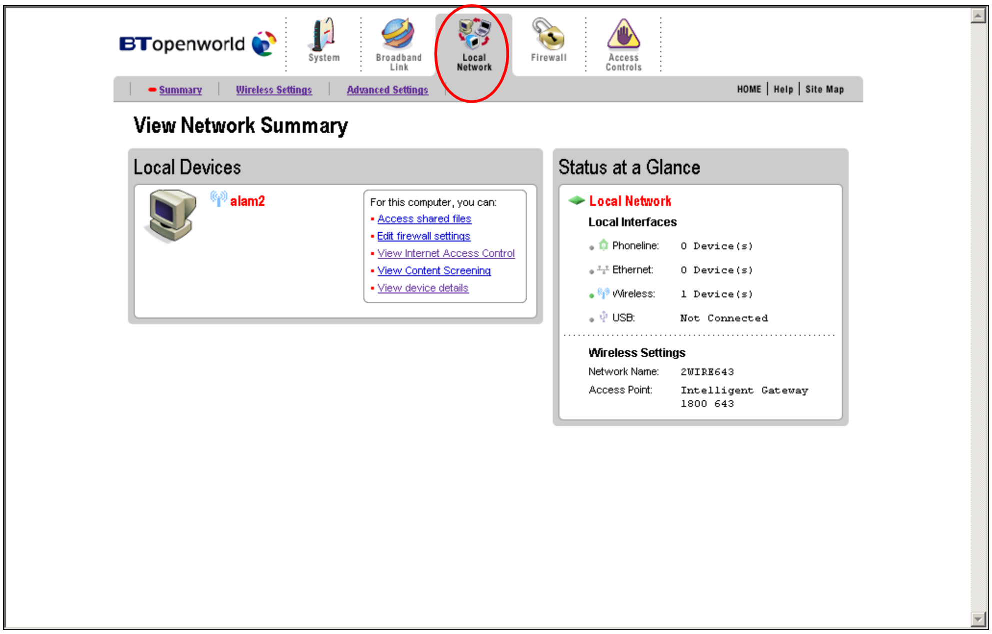
- View available upgrades and options

Set Up

Run the System Setup Wizard.

- Registration info
- Run System Setup Wizard

2. Click the Local Network tab.



View Network Summary

Local Devices

alam2

For this computer, you can:
- Access shared files
- Edit firewall settings
- View Internet Access Control
- View Content Screening
- View device details

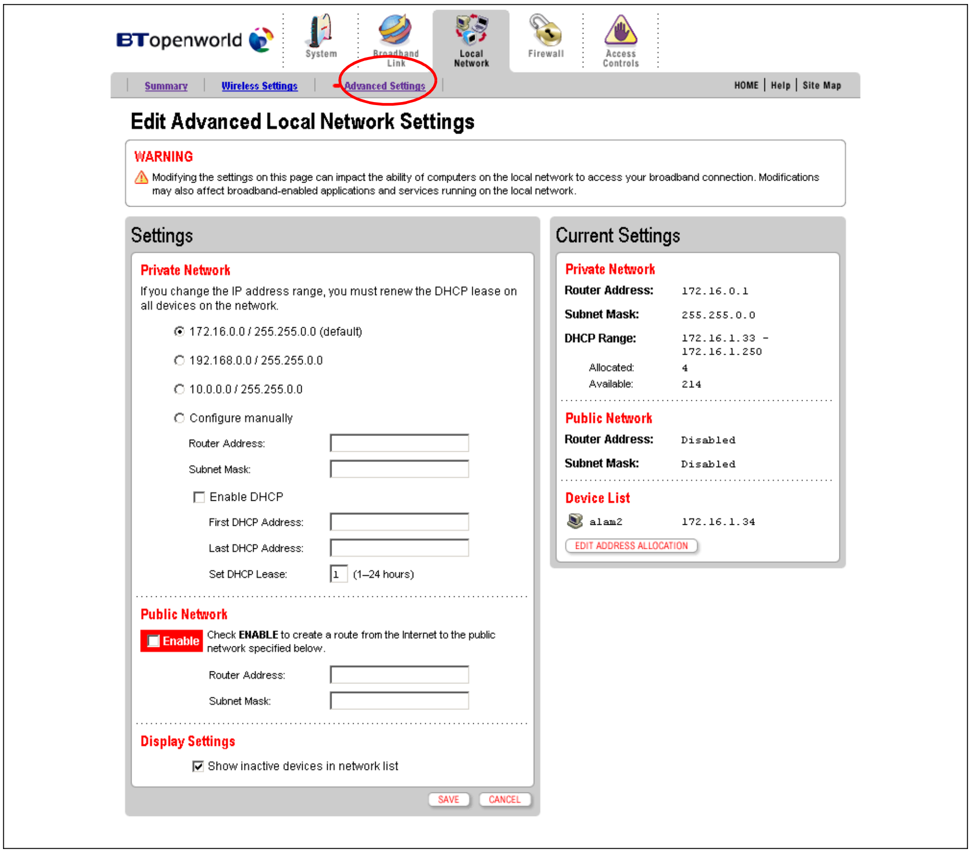
Status at a Glance

Local Network
Local Interfaces

- Phoneline: 0 Device(s)
- Ethernet: 0 Device(s)
- Wireless: 1 Device(s)
- USB: Not Connected

Wireless Settings
Network Name: 2WIRE643
Access Point: Intelligent Gateway 1800 643

3. Click Advanced Settings.



Edit Advanced Local Network Settings

WARNING

Modifying the settings on this page can impact the ability of computers on the local network to access your broadband connection. Modifications may also affect broadband-enabled applications and services running on the local network.

Settings

Private Network

If you change the IP address range, you must renew the DHCP lease on all devices on the network.

● 172.16.0.0 / 255.255.0.0 (default)

○ 192.168.0.0 / 255.255.0.0

○ 10.0.0.0 / 255.255.0.0

○ Configure manually

Router Address:

Subnet Mask:

□ Enable DHCP

First DHCP Address:

Last DHCP Address:

Set DHCP Lease: 1 (1–24 hours)

Public Network

□ Enable Check **ENABLE** to create a route from the Internet to the public network specified below.

Router Address:

Subnet Mask:

Display Settings

☑ Show inactive devices in network list

Current Settings

Private Network

Router Address:	172.16.0.1
Subnet Mask:	255.255.0.0
DHCP Range:	172.16.1.33 – 172.16.1.250
Allocated:	4
Available:	214

Public Network

Router Address:	Disabled
Subnet Mask:	Disabled

Device List

alan2	172.16.1.34

4. In the Settings pane, increase the DHCP timeout period to 24 hours by entering “24” in the **Set DHCP Lease** field.

5. Click the **SAVE** button.

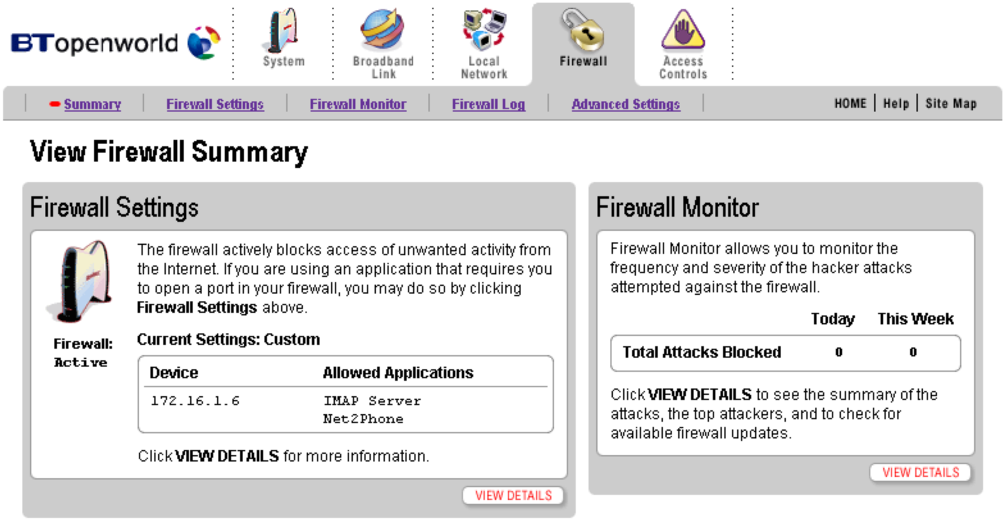
As an alterantive to increasing the DHCP timeout, you can assign static IP addresses to the computer. Because the method for assigning static IP addresses depends on the computer operating system, refer to the documentation that came with your computer.

Firewall

The Intelligent Gateway incorporates a professional-grade firewall to help deter outside “hackers” from accessing your local network. The Firewall pages provide access to your system security settings, and allow you to configure your firewall.

Viewing your firewall summary

The Summary page provides summary information and links to the most commonly used security-related features of your system. The Firewall Settings panel shows you how the firewall is configured. The system’s firewall software filters and blocks data coming in from the Internet that could be harmful to your network. You can configure the firewall to allow specific application traffic from the Internet to pass through to a computer on your local network.



View Firewall Summary

Firewall Settings

The firewall actively blocks access of unwanted activity from the Internet. If you are using an application that requires you to open a port in your firewall, you may do so by clicking **Firewall Settings** above.

Current Settings: Custom

Device	Allowed Applications
172.16.1.6	IMAP Server Net2Phone

Click **VIEW DETAILS** for more information.

Firewall Monitor

Firewall Monitor allows you to monitor the frequency and severity of the hacker attacks attempted against the firewall.

	Today	This Week
Total Attacks Blocked	0	0

Click **VIEW DETAILS** to see the summary of the attacks, the top attackers, and to check for available firewall updates.

If the firewall has been configured to allow traffic from the Internet to pass through, the device and the allowed application are listed. If application traffic is allowed, external users on the Internet can have limited access to your local network. This access might be required in order for some programs such as game servers and messaging software to operate properly. For example, a remote game player on the Internet might need to contact the game server program that you have installed on your local network in order to play against you. Normally, the firewall blocks this communication. By changing the firewall settings, this communication is permitted to pass through a “pinhole” in the firewall. This function may be referred to as “port-mapping” or “port-forwarding” in your software program documentation.

A status message displays the firewall’s Current Settings. The default settings disallow all unsolicited inbound traffic to provide maximum protection for your local network. The Current Settings will be displayed as “Custom” if any applications have been associated with computers on your network.

The summary displays an access list showing the computers (“Devices”) on your network and the names of the Allowed Applications for each computer.

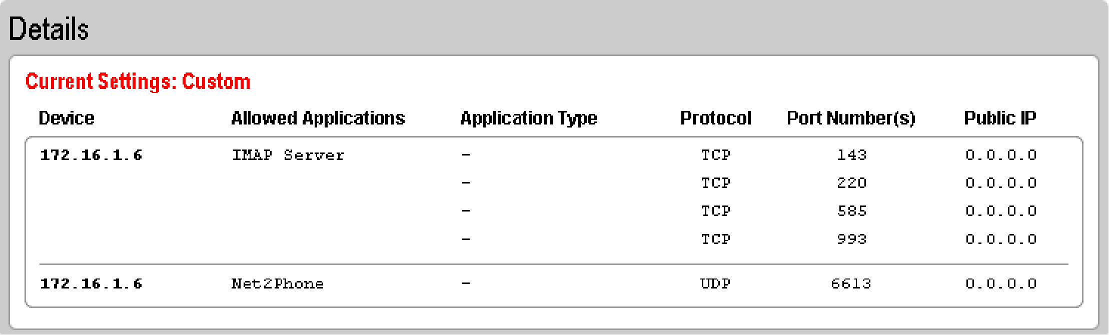
Click **VIEW DETAILS** to access the Firewall Details page, which shows a list of all the devices that have applications configured in the firewall and the details of these configurations.

Viewing firewall details

The Firewall Details page displays the details of all the applications allowed to pass through the firewall, and includes the following information:

- **Application Type.** A special set of rules required by complex applications to ensure that all of the necessary data is passed correctly through the firewall.
- **Protocol.** The Internet protocol used by the application to send and receive data. Data that is transferred over the Internet must conform to one of a number of defined standards. This column indicates the protocol used by the data for the firewall to properly forward the data to the assigned computer. An application may require multiple protocols to communicate.
- **Port Numbers.** Some Internet protocols transfer data through specific channels or connection numbers known as ports. For example, an instant messenger application may send a message using

the TCP protocol and Port 2999. The system recognizes that the data on Port 2999 (or a range of ports) is required for the specified application, and routes it accordingly.



Details

Current Settings: Custom

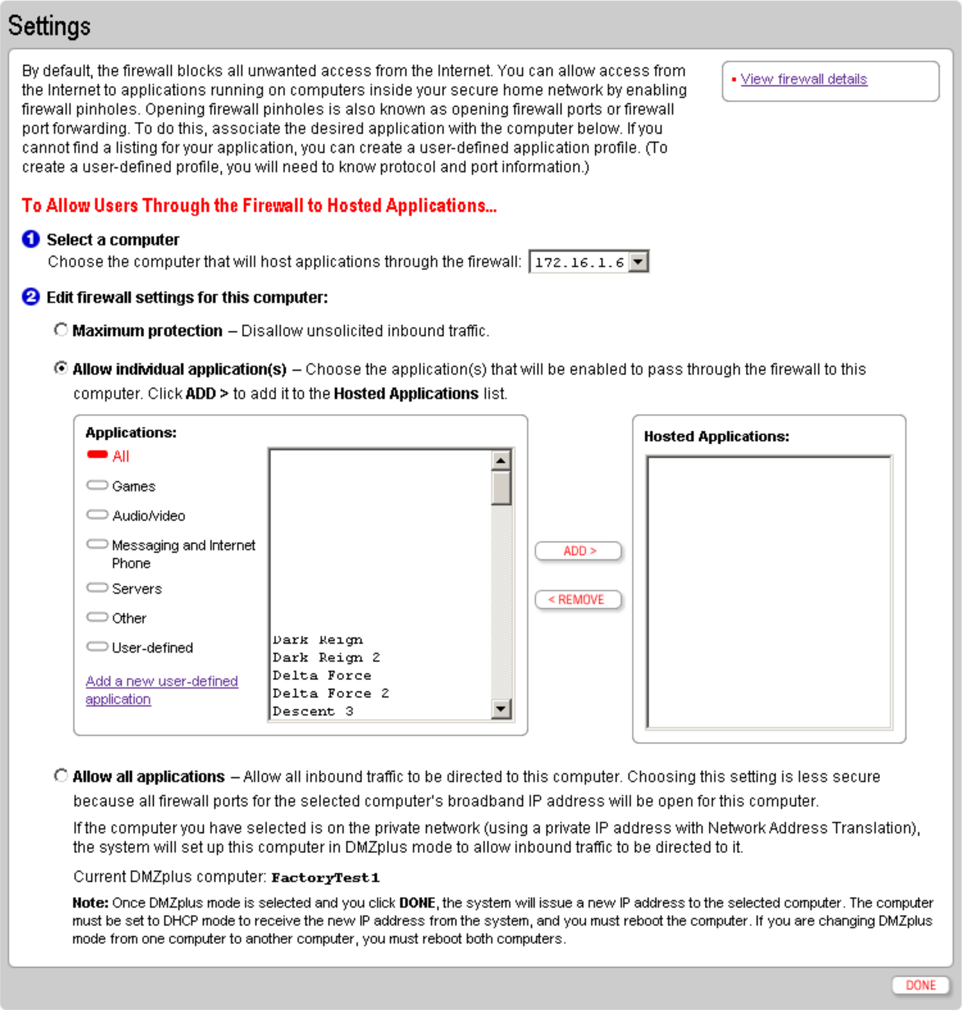
Device	Allowed Applications	Application Type	Protocol	Port Number(s)	Public IP
172.16.1.6	IMAP Server	-	TCP	143	0.0.0.0
		-	TCP	220	0.0.0.0
		-	TCP	585	0.0.0.0
		-	TCP	993	0.0.0.0
172.16.1.6	Net2Phone	-	UDP	6613	0.0.0.0

Click **EDIT SETTINGS** to access a page where you can map an application to a computer that will allow traffic through the firewall.

The Firewall Monitor panel provides a summary of recent attacks blocked by your firewall. Click **VIEW DETAILS** to access the main Firewall Monitor page, which displays more detailed information about recent firewall attacks, information about your firewall rule database, and your attack alert settings.

Editing your firewall settings

The Firewall Settings page allows you to configure the firewall to pass through specific application data to a selected computer.



Settings

By default, the firewall blocks all unwanted access from the Internet. You can allow access from the Internet to applications running on computers inside your secure home network by enabling firewall pinholes. Opening firewall pinholes is also known as opening firewall ports or firewall port forwarding. To do this, associate the desired application with the computer below. If you cannot find a listing for your application, you can create a user-defined application profile. (To create a user-defined profile, you will need to know protocol and port information.)

- View firewall details

To Allow Users Through the Firewall to Hosted Applications...

1 **Select a computer**
Choose the computer that will host applications through the firewall: 172.16.1.6

2 **Edit firewall settings for this computer:**

○ **Maximum protection** – Disallow unsolicited inbound traffic.

● **Allow individual application(s)** – Choose the application(s) that will be enabled to pass through the firewall to this computer. Click **ADD >** to add it to the **Hosted Applications** list.

○ **Allow all applications** – Allow all inbound traffic to be directed to this computer. Choosing this setting is less secure because all firewall ports for the selected computer's broadband IP address will be open for this computer.

If the computer you have selected is on the private network (using a private IP address with Network Address Translation), the system will set up this computer in DMZplus mode to allow inbound traffic to be directed to it.

Current DMZplus computer: **FactoryTest1**

Note: Once DMZplus mode is selected and you click **DONE**, the system will issue a new IP address to the selected computer. The computer must be set to DHCP mode to receive the new IP address from the system, and you must reboot the computer. If you are changing DMZplus mode from one computer to another computer, you must reboot both computers.

If you want to host an application on your network for Internet users to access (such as a Web server), you must configure your firewall to allow users on the Internet to access it. To do so:

1. From the Select a computer pull-down menu, select the computer.
2. Select the **Allow individual application(s)** radio button.
3. Select an application profile.
4. Click the **ADD >** button.
5. Click the **DONE** button.

Note: *The applications can be sorted by category. To choose a category, click the oval next to the category name. Click* **ALL** *to see a list of all the application profiles.*

To stop an application that is routed to a selected computer:

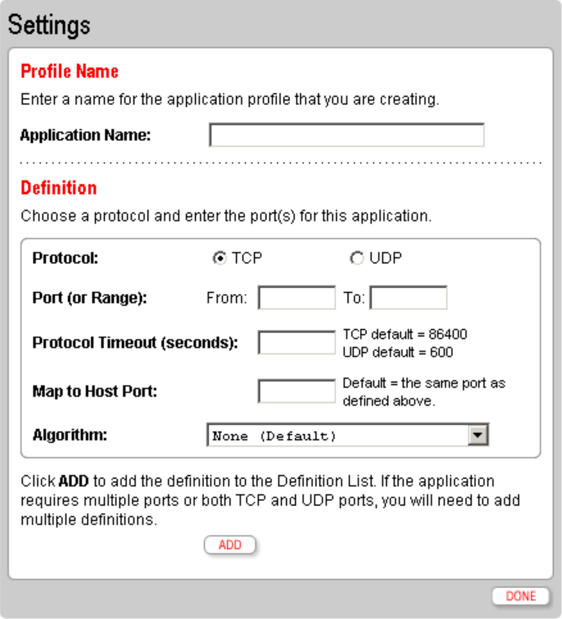
1. Select the application profile name from the Hosted Applications list.
2. Click the **< REMOVE** button.

Updating your Application Profile list

If the application you want to host does not appear in the Application Profile list, you may need to update your application list. If an update is available, click the **UPDATE APPLICATION LIST** button above the list of application profiles.

Creating, editing, or deleting your Application Profile

If the application that you want to host is not included in the updated application list, you may need to create your own application profile. An application profile configures your system's firewall to pass through application-specific data. This feature is typically used if the application for which you would like to pass through data to a given computer is new or has been recently updated to a new version.



Settings

Profile Name

Enter a name for the application profile that you are creating.

Application Name:

Definition

Choose a protocol and enter the port(s) for this application.

Protocol: ● TCP ○ UDP

Port (or Range): From: To:

Protocol Timeout (seconds): TCP default = 86400 UDP default = 600

Map to Host Port: Default = the same port as defined above.

Algorithm: None (Default)

Click **ADD** to add the definition to the Definition List. If the application requires multiple ports or both TCP and UDP ports, you will need to add multiple definitions.

To create an application profile:

1. Click the **Add a new user-defined application** link. The Edit Application page opens.
2. In the Application Name field, enter a name for the application profile. We recommend that you use the name of the application, such as "ICIMI Messenger" or "Redwing Game Server."
3. In the Protocol field, click the **TCP** or **UDP** radio button. If both protocols are required, you must create a definition for each.
4. In the Port (or Range) field, enter the port or port range used by the application.
5. In the Protocol Timeout (seconds) field, enter the amount of time (in seconds) that the connection in the specified range should remain open when there is no data transfer. This is an advanced feature, and in most cases the default value is appropriate.
6. In the Map to Host Port field, enter the value that provides the mapping offset to the local computer. For example, if this value is set to 4000 and the range being opened is 100 to 108, the forwarded data to the first value in the range will be sent to 4000. Subsequent ports will be mapped accordingly; 101 will be sent to 4001, 102 will be sent to 4002, etc.
7. Click **ADD** to add the values entered to the profile definition list at the bottom of the screen. You must click **ADD** to retain the defined values.

8. Repeat the previous step for each port or range of ports required for the application profile.

9. Click **DONE**.

To edit application profiles that you have created, select the profile from the list and click the **EDIT** button. This launches the Edit Application Profile panel.

To delete an application profile, select the application profile from the list and click **DELETE**.

Allowing all applications

DMZplus is a special firewall mode that is used for hosting applications if an application will not operate properly using the "Allow individual application(s)" option. When in DMZplus mode, the designated computer:

- Shares your Router Address (the Intelligent Gateway IP address).
- Appears as if it is directly connected to the Internet.
- Has all of the unassigned TCP and UDP ports opened and pointed to it.
- Can receive unsolicited network traffic from the Internet.

Note: *Although the DMZplus computer appears to Internet users as though it is directly connected to the Internet, it is still protected by your system firewall. All traffic is inspected by the firewall's Stateful Packet Inspection engine and all known hacker attacks continue to be blocked.*

Because all filtered traffic is forwarded to the designated computer, DMZplus mode should be used with caution. In most situations, you can use the "Allow individual application(s)" option to support access from the Internet to applications on your network.

Note: *DMZplus can only be configured for one computer on your local network at a time.*

To configure a computer on your network for DMZplus mode:

1. Select the computer to which you wish to have all data sent.

2. Click the **Allow all applications** radio button.

3. Click **DONE**.

4. Access the selected computer.

5. Confirm that the computer is configured for DHCP. If it is not, configure it for DHCP.

6. Restart the computer.

When the computer restarts, it receives a special IP address from the system and all unassigned TCP and UDP ports are forwarded to it.

To disable DMZplus mode:

1. Select the computer for which you wish to disable DMZplus.
2. Select **Maximum protection**.
3. Click **DONE**.
4. Access the computer that is in DMZplus mode.
5. If the computer will continue to automatically obtain an IP address, restart the computer. If the computer will have a static IP address, configure it with a valid static IP address and then restart it.

Monitoring the firewall

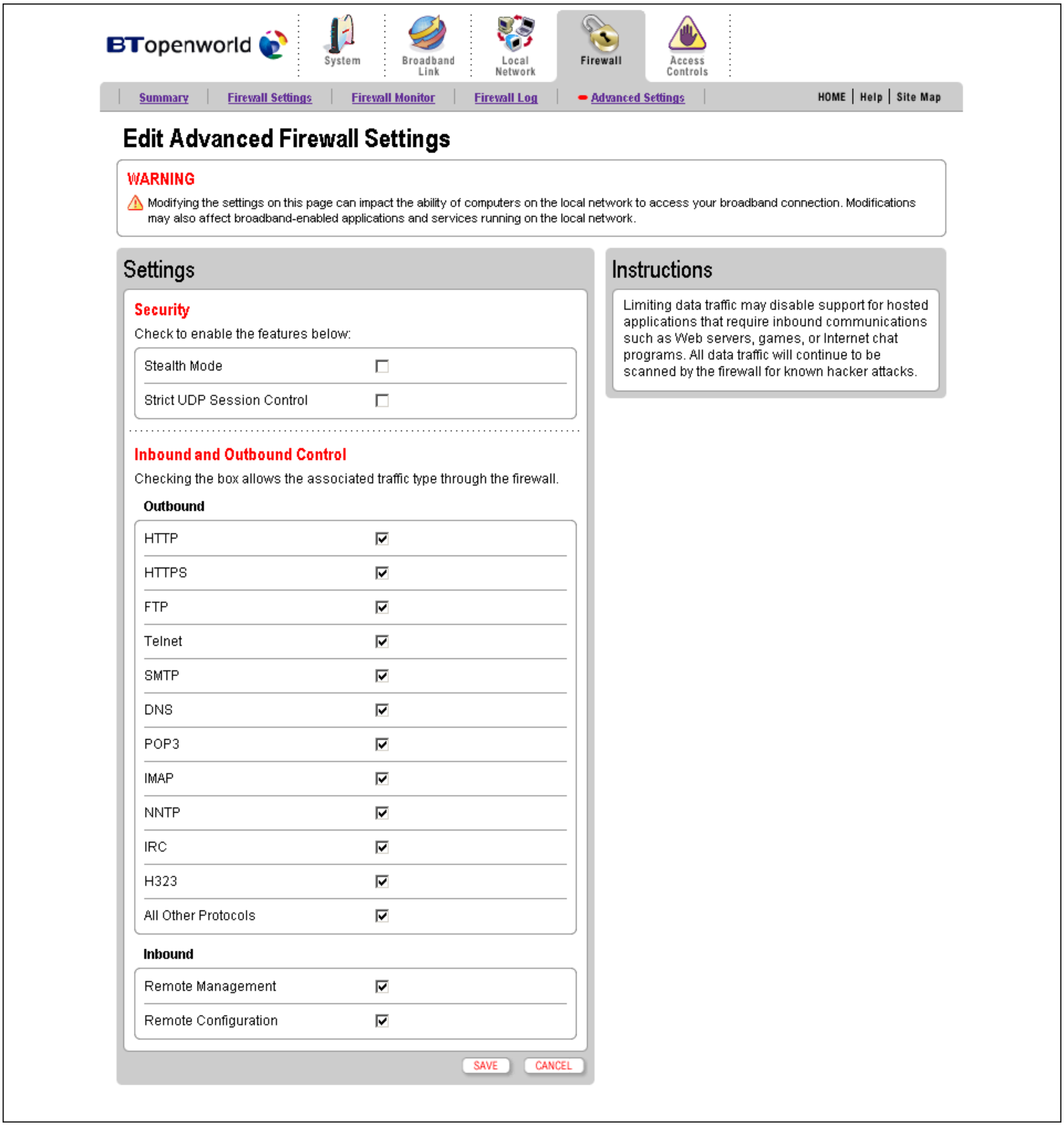
The Firewall Monitor enhanced service extends the professional-grade firewall capabilities of your system by continuously assessing threats to your local network. The Firewall Monitor enhanced service allows you to:

- Automatically download updates to your firewall software to protect against new threats.
- Receive on-screen or email notification to alert you of network attacks.
- Review details about attacks blocked and the source of the attacks.

Refer to the Firewall Monitor chapter for detailed information on using the Firewall Monitor enhanced service.

Editing advanced firewall settings

Advanced firewall configuration allows advanced users to further configure the system software firewall. You should use this feature only if you have advanced knowledge about firewalls and networking.



Edit Advanced Firewall Settings

WARNING

Modifying the settings on this page can impact the ability of computers on the local network to access your broadband connection. Modifications may also affect broadband-enabled applications and services running on the local network.

Settings

Security

Check to enable the features below:

Stealth Mode	□
Strict UDP Session Control	□

Inbound and Outbound Control

Checking the box allows the associated traffic type through the firewall.

Outbound

HTTP	☑
HTTPS	☑
FTP	☑
Telnet	☑
SMTP	☑
DNS	☑
POP3	☑
IMAP	☑
NNTP	☑
IRC	☑
H323	☑
All Other Protocols	☑

Inbound

Remote Management	☑
Remote Configuration	☑

Instructions

Limiting data traffic may disable support for hosted applications that require inbound communications such as Web servers, games, or Internet chat programs. All data traffic will continue to be scanned by the firewall for known hacker attacks.

If an Inbound box is checked, the firewall allows the corresponding protocol to pass through from the Internet to the network. If an Outbound box is checked, the firewall allows the traffic from the network to pass through the firewall to the Internet. You must click **SAVE** for the changes to take effect.

Note: *Allowing inbound traffic does not mean that the firewall automatically allows this type of traffic to pass through the firewall to the network. Even if a particular protocol/application type is allowed via the Advanced Configuration settings, the firewall still checks and blocks all unsolicited traffic from the Internet unless the firewall is configured to allow the traffic through using an application profile.*

Note: *Firewall filtering takes precedence over application hosting. If you disable the incoming traffic, you may disable support for hosted applications that require that type of inbound communication.*

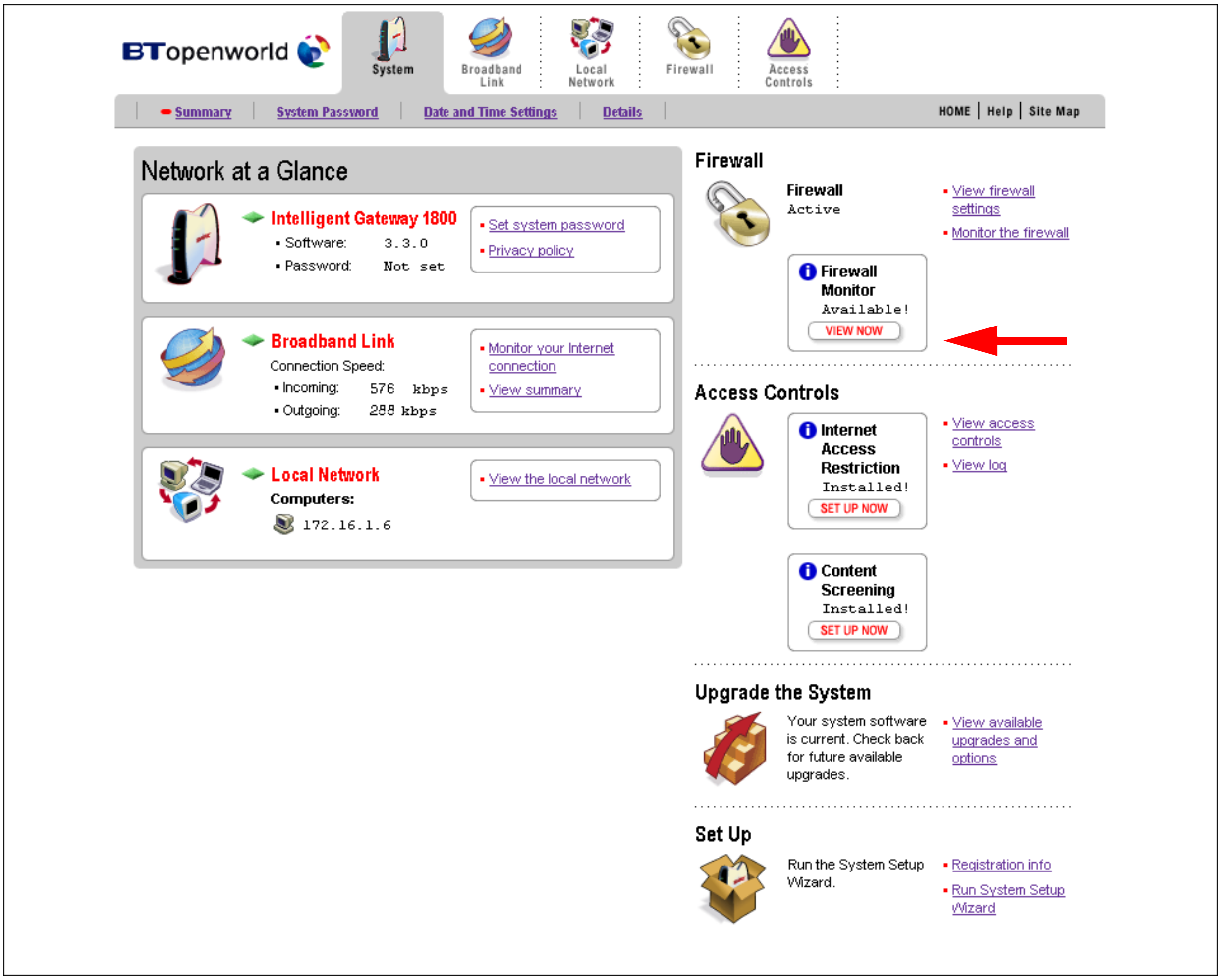
Firewall Monitor

The Firewall Monitor enhanced service extends the professional-grade firewall capabilities of your Intelligent Gateway by continuously assessing threats to your home network. Using the Firewall Monitor service, you can:

- Automatically download updates to your firewall software to protect against new threats.
- Receive on-screen notification to alert you of network attacks.
- Review details about attacks blocked and the source of the attacks.

Setting up Firewall Monitor attack alerts

The Attack Alerts area of the Monitor Your Firewall page shows you the current criteria for posting an alert and how you will be notified of the attack.



Network at a Glance

Intelligent Gateway 1800
- Software: 3.3.0
- Password: Not set

- Set system password
- Privacy policy

Broadband Link
Connection Speed:
- Incoming: 576 kbps
- Outgoing: 288 kbps

- Monitor your Internet connection
- View summary

Local Network
Computers:
172.16.1.6

- View the local network

Firewall

Firewall
Active

- View firewall settings
- Monitor the firewall

Firewall Monitor
Available!
VIEW NOW

Access Controls

Internet Access Restriction
Installed!
SET UP NOW

Content Screening
Installed!
SET UP NOW

- View access controls
- View log

Upgrade the System

Your system software is current. Check back for future available upgrades.

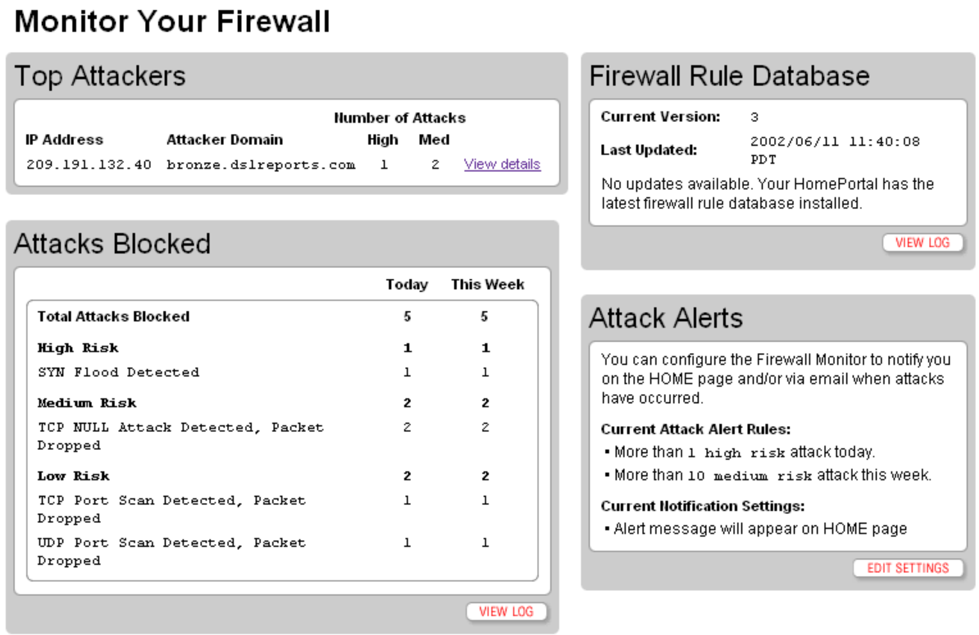
- View available upgrades and options

Set Up

Run the System Setup Wizard.

- Registration info
- Run System Setup Wizard

Click the **VIEW NOW** button to display the Monitor Your Firewall page where you can customize these settings for your firewall.



Monitor Your Firewall

Top Attackers

IP Address	Attacker Domain	Number of Attacks High	 Med	
209.191.132.40	bronze.dslreports.com	1	2	View details

Attacks Blocked

	Today	This Week
Total Attacks Blocked	5	5
High Risk	1	1
SYN Flood Detected	1	1
Medium Risk	2	2
TCP NULL Attack Detected, Packet Dropped	2	2
Low Risk	2	2
TCP Port Scan Detected, Packet Dropped	1	1
UDP Port Scan Detected, Packet Dropped	1	1

VIEW LOG

Firewall Rule Database

Current Version: 3

Last Updated: 2002/06/11 11:40:08 PDT

No updates available. Your HomePortal has the latest firewall rule database installed.

VIEW LOG

Attack Alerts

You can configure the Firewall Monitor to notify you on the HOME page and/or via email when attacks have occurred.

Current Attack Alert Rules:

- More than 1 high risk attack today.
- More than 10 medium risk attack this week.

Current Notification Settings:

- Alert message will appear on HOME page

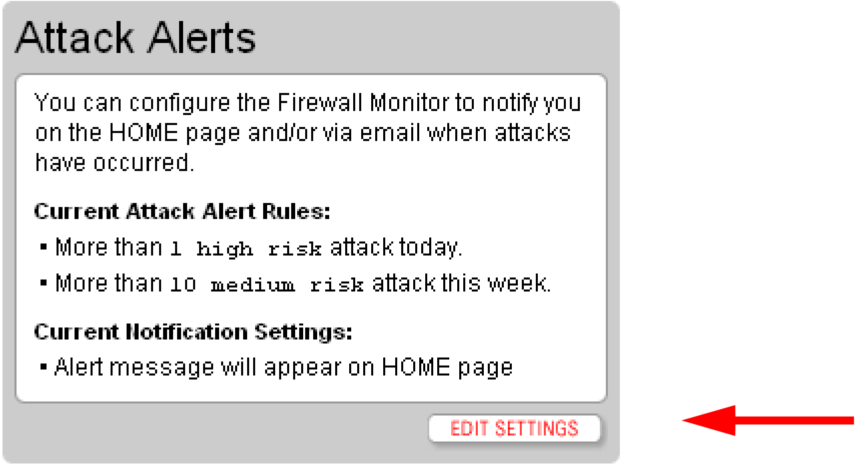
EDIT SETTINGS

The Monitor Your Firewall page contains four areas:

- Top Attackers
- Attacks Blocked
- Firewall Rule Database
- Attack Alerts

Configuring/editing attack alerts

To configure the Attack Alerts criteria, click **EDIT SETTINGS**.



Attack Alerts

You can configure the Firewall Monitor to notify you on the HOME page and/or via email when attacks have occurred.

Current Attack Alert Rules:

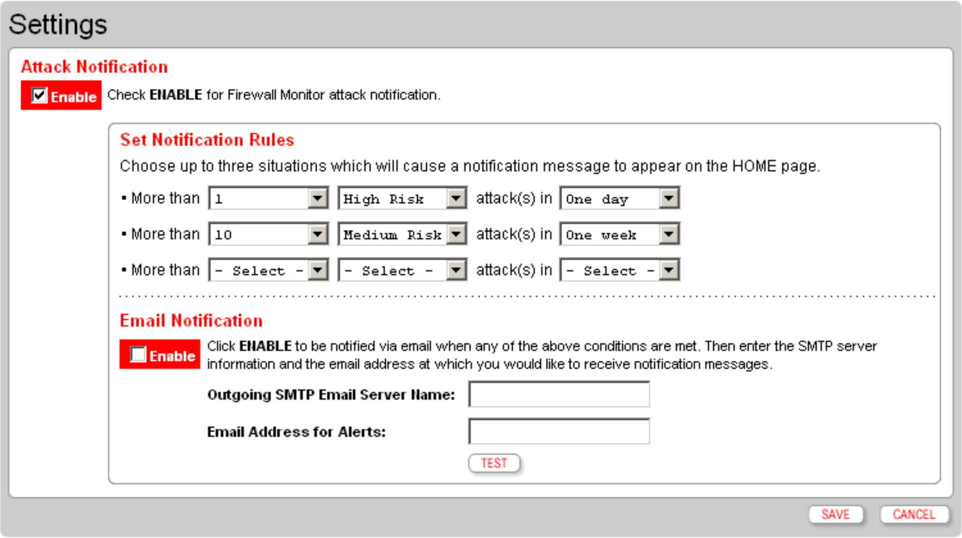
- More than 1 high risk attack today.
- More than 10 medium risk attack this week.

Current Notification Settings:

- Alert message will appear on HOME page

EDIT SETTINGS

The Edit Attack Notification Settings page opens.



Settings

Attack Notification

☑ Enable Check **ENABLE** for Firewall Monitor attack notification.

Set Notification Rules

Choose up to three situations which will cause a notification message to appear on the HOME page.

- More than 1 High Risk attack(s) in One day
- More than 10 Medium Risk attack(s) in One week
- More than - Select - - Select - attack(s) in - Select -

Email Notification

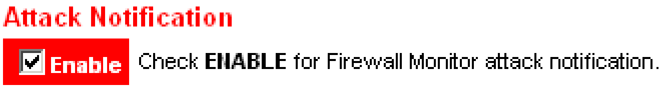
☐ Enable Click **ENABLE** to be notified via email when any of the above conditions are met. Then enter the SMTP server information and the email address at which you would like to receive notification messages.

Outgoing SMTP Email Server Name:

Email Address for Alerts:

Enabling attack notification

To enable the attack notification function, make sure the Attack Notification Enable checkbox is checked. If you wish to disable this function, uncheck the checkbox.



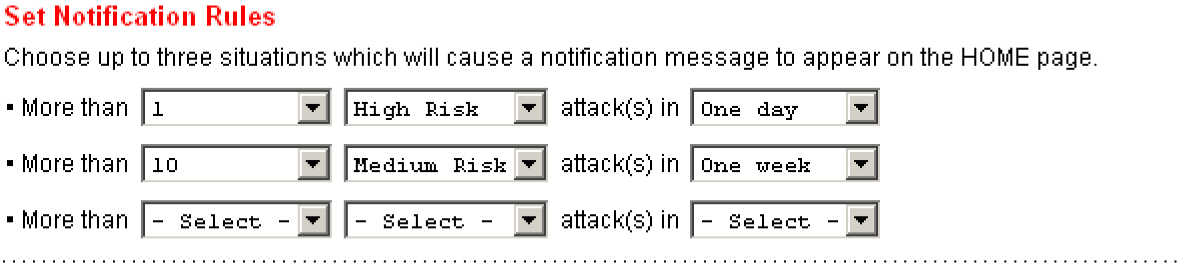
Attack Notification

☑ Enable Check **ENABLE** for Firewall Monitor attack notification.

When you are finished setting your attack notification criteria, click **SAVE** for your notifications rules to take effect.

Configuring notification rules

To be notified of attacks on the Intelligent Gateway home page, you must set up notification rules. You can configure up to three notification rules that will cause a notification message to appear on the Intelligent Gateway home page. The following screen shows the default rules.



Set Notification Rules

Choose up to three situations which will cause a notification message to appear on the HOME page.

- More than 1 High Risk attack(s) in One day
- More than 10 Medium Risk attack(s) in One week
- More than - Select - - Select - attack(s) in - Select -

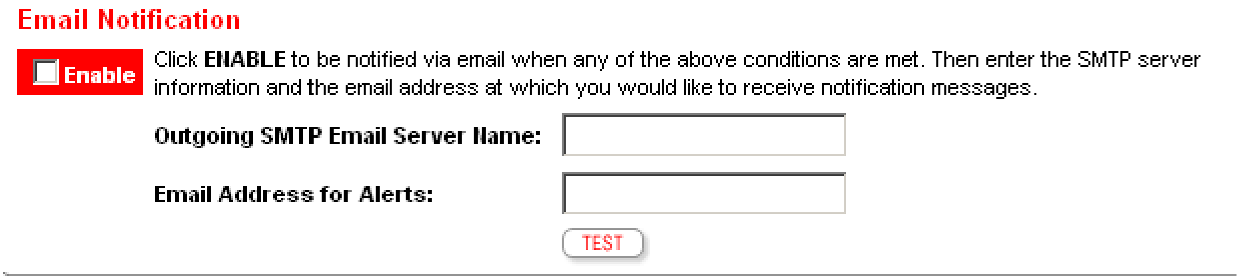
Each rule contains the following parameters:

- Number of Attacks. Select the quantity of attacks that have to occur before the notification is sent. Choices include 1, 5, 10, 15, 25, 50, and 100 attacks.
- Type of Attack. Select the type of attack for this notification rule. Choices include high risk, medium risk, and low risk attacks. Refer to the Viewing top attackers section for a definition of attack categories.

- Time Duration. Select the time duration. If the number of attacks specified is exceeded within the chosen duration, you are notified. Choices include one day or one week. A week is defined as Monday at midnight to Sunday at midnight.

Enabling email notification

In addition to being notified of attacks on the Intelligent Gateway home page, you can be notified via email when one of your attack threshold rules has been exceeded. To receive an email notification when any of the Notification Rule conditions have been met, check the Email Notification Enable checkbox. You must also enter your Outgoing SMTP Email Server Name and the email address that will receive the alerts.



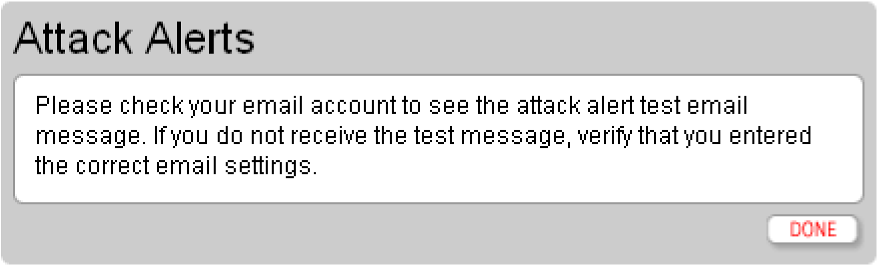
Email Notification

☐ Enable Click **ENABLE** to be notified via email when any of the above conditions are met. Then enter the SMTP server information and the email address at which you would like to receive notification messages.

Outgoing SMTP Email Server Name:

Email Address for Alerts:

To test the email information, click **TEST**. You are prompted with a message indicating that your test message has been sent.



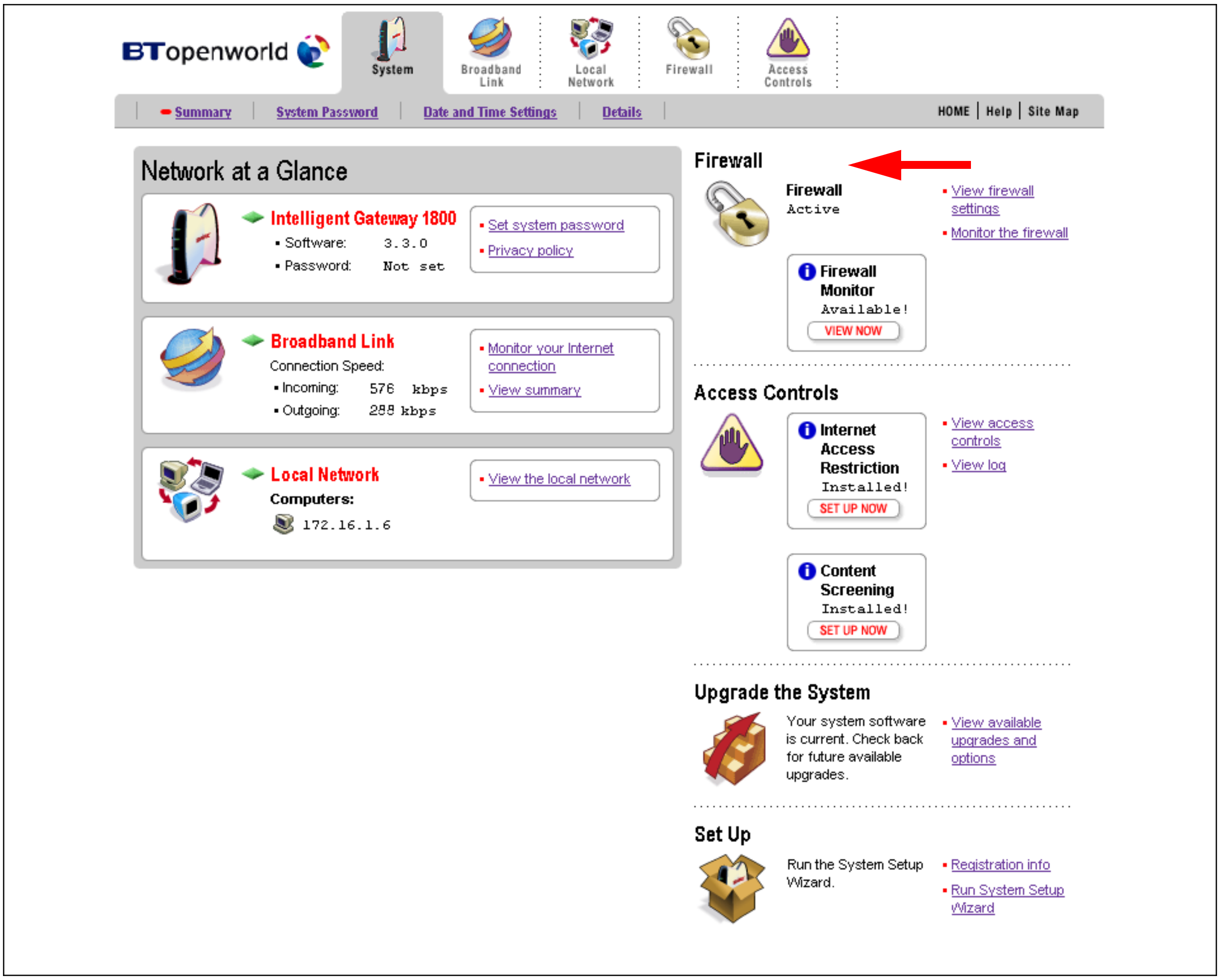
Attack Alerts

Please check your email account to see the attack alert test email message. If you do not receive the test message, verify that you entered the correct email settings.

Click **DONE** to be returned to the Monitor Your Firewall page.

Viewing Firewall Monitor attack alerts

After setting up alert notification, if your network firewall is attacked meeting the criteria set, notice of the attack is provided on the Intelligent Gateway home page, in the Firewall area.



Network at a Glance

Intelligent Gateway 1800
- Software: 3.3.0
- Password: Not set

Broadband Link
Connection Speed:
- Incoming: 576 kbps
- Outgoing: 288 kbps

Local Network
Computers:
172.16.1.6

Firewall

Firewall Active

Firewall Monitor Available!

Access Controls

Internet Access Restriction Installed!

Content Screening Installed!

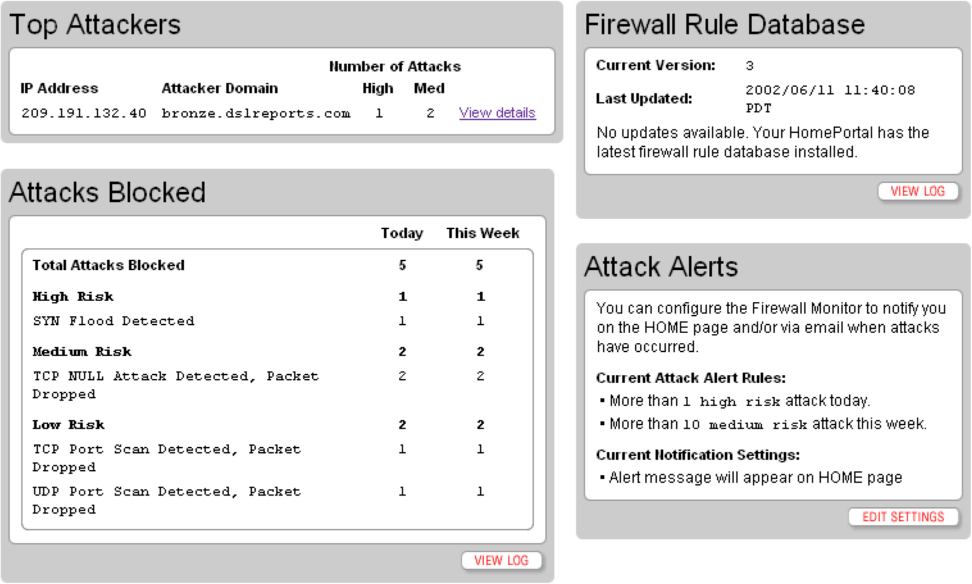
Upgrade the System

Your system software is current. Check back for future available upgrades.

Set Up

Run the System Setup Wizard.

Click the **VIEW NOW** button to display the Monitor Your Firewall page and view attacks made to your network firewall.



Top Attackers

		Number of Attacks		
IP Address	Attacker Domain	High	Med	
209.191.132.40	bronze.dslreports.com	1	2	View details

Attacks Blocked

	Today	This Week
Total Attacks Blocked	5	5
High Risk	1	1
SYN Flood Detected	1	1
Medium Risk	2	2
TCP NULL Attack Detected, Packet Dropped	2	2
Low Risk	2	2
TCP Port Scan Detected, Packet Dropped	1	1
UDP Port Scan Detected, Packet Dropped	1	1

Firewall Rule Database

Current Version: 3

Last Updated: 2002/06/11 11:40:08 PDT

No updates available. Your HomePortal has the latest firewall rule database installed.

Attack Alerts

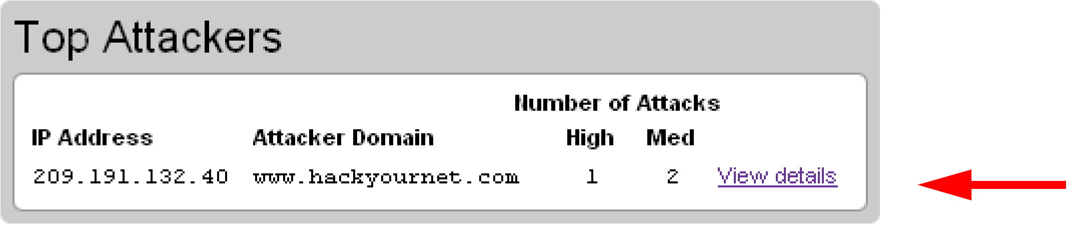
You can configure the Firewall Monitor to notify you on the HOME page and/or via email when attacks have occurred.

Current Attack Alert Rules:
- More than 1 high risk attack today.
- More than 10 medium risk attack this week.

Current Notification Settings:
- Alert message will appear on HOME page

Viewing top attackers

The Top Attackers area of the Monitor Your Firewall page displays the IP address and domain of each top attacker.

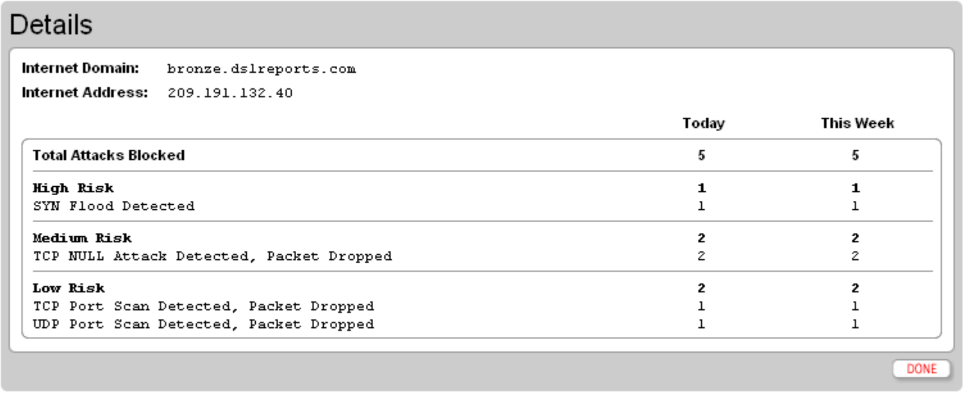


Top Attackers

		Number of Attacks		
IP Address	Attacker Domain	High	Med	
209.191.132.40	www.hackyournet.com	1	2	View details

The attackers are ranked based on the number and severity of attacks. To see the details of a particular top attacker, click the **View Details** link of the attacker you wish to view.

The View Attacker Details page opens.



Details

Internet Domain: bronze.dslreports.com
Internet Address: 209.191.132.40

	Today	This Week
Total Attacks Blocked	5	5
High Risk	1	1
SYN Flood Detected	1	1
Medium Risk	2	2
TCP NULL Attack Detected, Packet Dropped	2	2
Low Risk	2	2
TCP Port Scan Detected, Packet Dropped	1	1
UDP Port Scan Detected, Packet Dropped	1	1

The View Attacker Details page shows you the following attack categories and the number of each type of attack that was blocked today and this week:

- Total attacks blocked
- High risk attacks. Indicates blocked attacks that represent a serious attempt by the attacker to disable your network.
- Medium risk attacks. Indicates blocked attacks that represent a modest level of intent by the attacker to disable your network.
- Low risk attacks. Indicates blocked attacks that represent no serious threat to the network. Typically, these are probing attacks used by hackers to determine those networks on which a more serious attack will be conducted.

When you are finished viewing the log, click **DONE**.

Reporting attacks

Due to level of hacker activity on the Internet and the “always on” nature of broadband, it will be quite normal for the Firewall Monitor to report a number of port scans and potential attacks daily. These reports are a positive indication that your firewall is working and protecting your computers from attack.

Note: *The Intelligent Gateway firewall does not provide anti-virus protection. To fully protect your computers, we would advise you consider using anti-virus software (such as BT NetProtect) on each computer on your network.*

Your Firewall Monitor will give you details about each potential attack, including its source address. BT Openworld can ***ONLY*** investigate attacks that originate from our address space. Customers who originate attacks from our address space are not complying with our terms and conditions, and may have their account terminated.

If an attack originates from BT's address space, "BT" will be displayed in the attacker domain column in the Top Attackers List. To report an attack that originated from our address space, please copy and paste all of the details from your Firewall Log, including address, time, date, and precise details of the attack (for example, the port numbers that were scanned) and email to abuse@btopenworld.com.

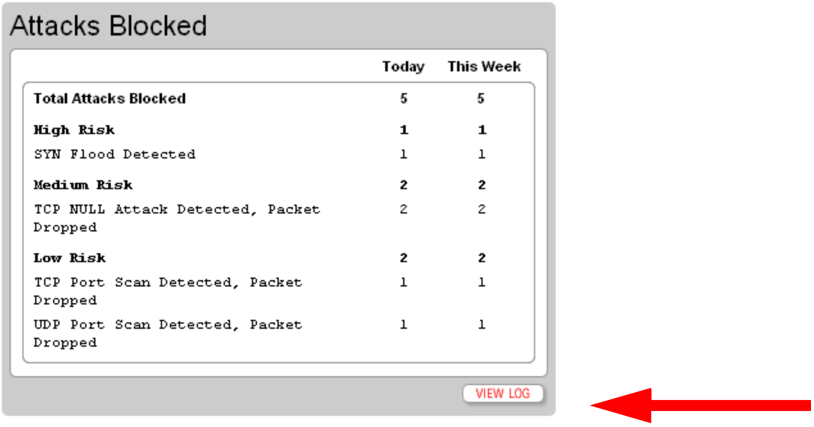
For attacks that originate from an address space other than BT Openworld, it is recommended that you directly contact the owner or service provider of the IP address or domain from which the attack originated to notify them of Internet abuse. You can determine the owner information by performing a reverse lookup on the IP address that is displayed in the Firewall Monitor log. For your convenience, you can use lookup tools on the World Wide Web to determine the owner of the displayed IP address, such as the free tool located at http://www.arin.net/whois.

It may also be necessary to look up the contact information for the owner/ provider so that you can contact them directly. You can search all domain name registrars at http://www.betterwhois.com.

You can also report the incident on a public Internet abuse web site. You can access several of these sites from links provided on http://www.doshelp.com.

Understanding the Attacks Blocked area

The Attacks Blocked area of the Monitor Your Firewall page displays summary information about all high, medium, and low risk attacks that were blocked today and this week.

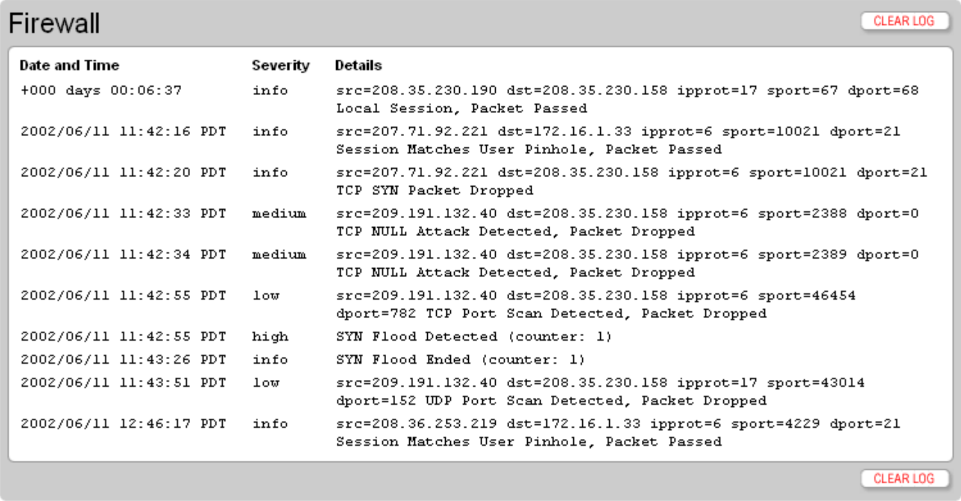


Attacks Blocked

	Today	This Week
Total Attacks Blocked	5	5
High Risk	**1**	**1**
SYN Flood Detected	1	1
Medium Risk	**2**	**2**
TCP NULL Attack Detected, Packet Dropped	2	2
Low Risk	**2**	**2**
TCP Port Scan Detected, Packet Dropped	1	1
UDP Port Scan Detected, Packet Dropped	1	1

To view details about the blocked attacks, click **VIEW LOG**.

The View Your Detailed Firewall Log page opens.



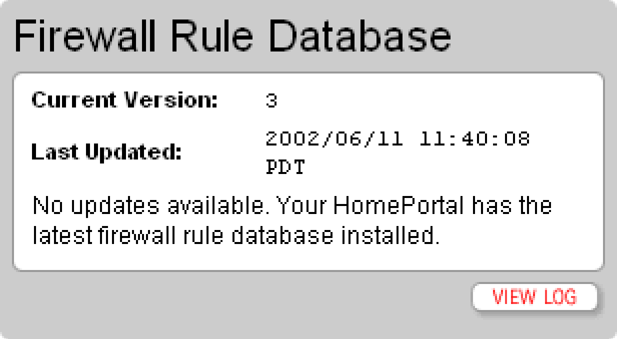
```
Date and Time            Severity  Details
+000 days 00:06:37       info      src=208.35.230.190 dst=208.35.230.158 ipprot=17 sport=67 dport=68
                                   Local Session, Packet Passed
2002/06/11 11:42:16 PDT  info      src=207.71.92.221 dst=172.16.1.33 ipprot=6 sport=10021 dport=21
                                   Session Matches User Pinhole, Packet Passed
2002/06/11 11:42:20 PDT  info      src=207.71.92.221 dst=208.35.230.158 ipprot=6 sport=10021 dport=21
                                   TCP SYN Packet Dropped
2002/06/11 11:42:33 PDT  medium    src=209.191.132.40 dst=208.35.230.158 ipprot=6 sport=2388 dport=0
                                   TCP NULL Attack Detected, Packet Dropped
2002/06/11 11:42:34 PDT  medium    src=209.191.132.40 dst=208.35.230.158 ipprot=6 sport=2389 dport=0
                                   TCP NULL Attack Detected, Packet Dropped
2002/06/11 11:42:55 PDT  low       src=209.191.132.40 dst=208.35.230.158 ipprot=6 sport=46454
                                   dport=782 TCP Port Scan Detected, Packet Dropped
2002/06/11 11:42:55 PDT  high      SYN Flood Detected (counter: 1)
2002/06/11 11:43:26 PDT  info      SYN Flood Ended (counter: 1)
2002/06/11 11:43:51 PDT  low       src=209.191.132.40 dst=208.35.230.158 ipprot=17 sport=43014
                                   dport=152 UDP Port Scan Detected, Packet Dropped
2002/06/11 12:46:17 PDT  info      src=208.36.253.219 dst=172.16.1.33 ipprot=6 sport=4229 dport=21
                                   Session Matches User Pinhole, Packet Passed
```

To clear the log, click **CLEAR LOG**.

To return to the Monitor Your Firewall page, click your browser **BACK** button.

Understanding the Firewall Rule Database area

The Firewall Rule Database area of the Monitor Your Firewall page shows you the current firewall rules version running on your Intelligent Gateway. It also shows you when the rules were last updated.

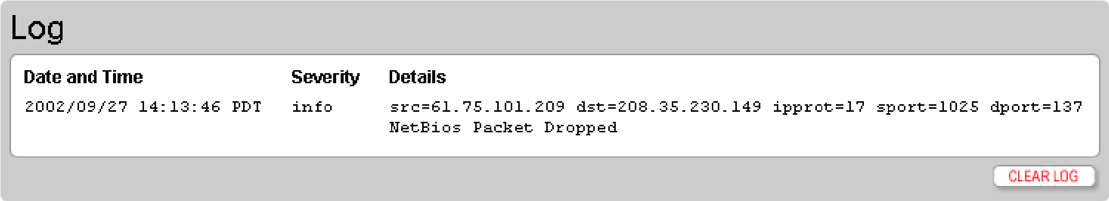


Current Version: 3

Last Updated: 2002/06/11 11:40:08 PDT

No updates available. Your HomePortal has the latest firewall rule database installed.

To display the firewall rule database update log, click **VIEW LOG**.



```
Date and Time            Severity  Details
2002/09/27 14:13:46 PDT  info      src=61.75.101.209 dst=208.35.230.149 ipprot=17 sport=1025 dport=137
                                   NetBios Packet Dropped
```

The upgrade log displays the following information about new downloaded rules:

- Date and time
- Version

When you are finished viewing the log, click **CLEAR LOG**.

Updating your firewall rules

Updated firewall rules are automatically downloaded to your Intelligent Gateway after you purchase the Firewall Monitor service. The Firewall Monitor application typically checks for new updates every 24 hours.

Access Controls

Access Controls combines two full-featured applications that create an easy-to-use solution to keep your office running smoothly:

- Internet Access Restriction
- Content Screening

Access Controls provides whole-network service. The password protected restrictions and schedules you set are managed at the Intelligent Gateway rather than through individual PCs. A default setting can be set for any new computers added to the network, so if an employee brings a home computer into the office, the restrictions are automatically in place.

Internet Access Restriction

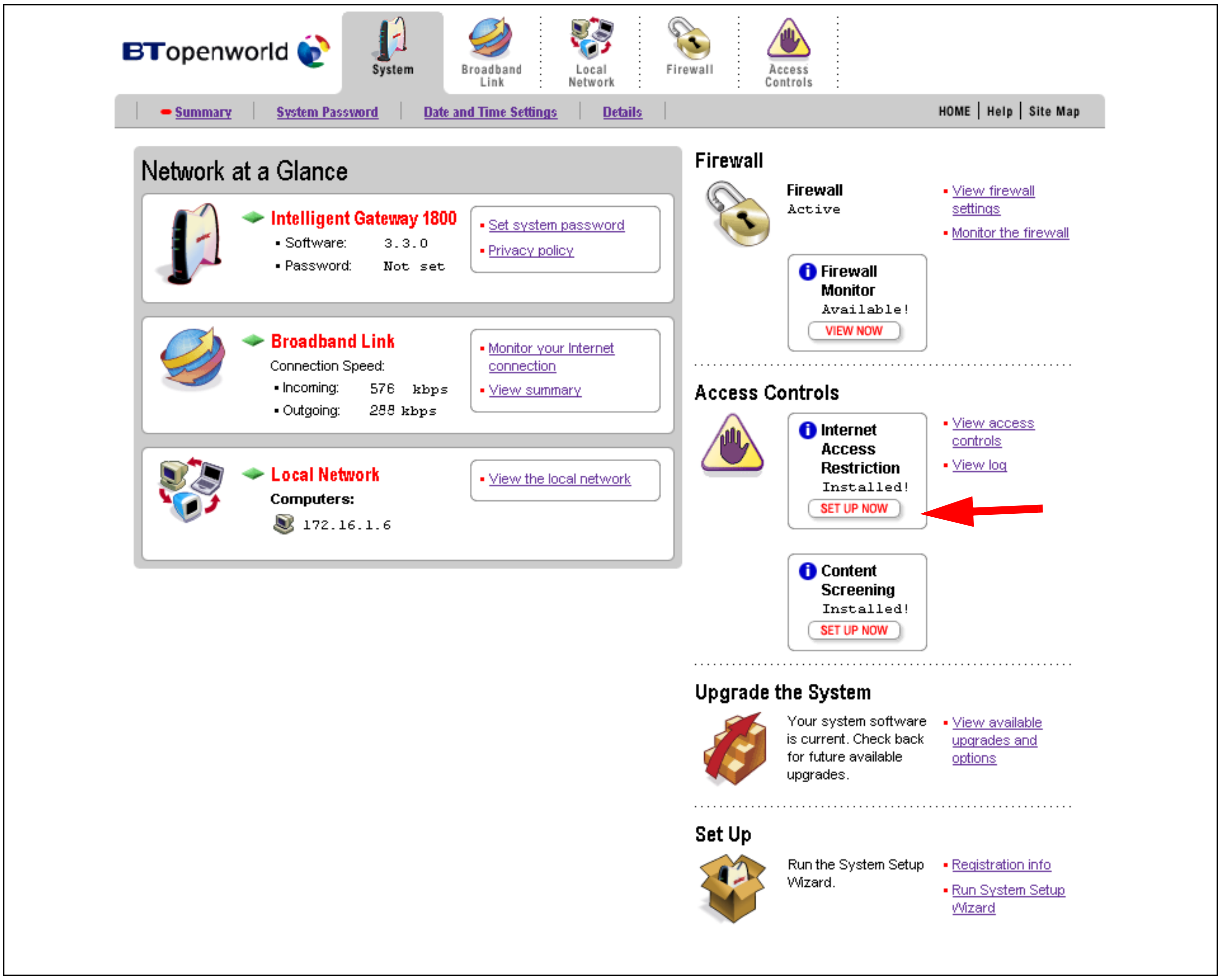
Internet Access Restriction allows you to:

- Set up employee profiles to block Internet usage based on day of week and time of day.
- Create Internet usage schedules for each computer in your business.
- Control the use of certain applications per user (such as Web browsing, Instant Messenger, and other Internet applications).

This level of control enables employers to ensure that employees are focusing only on business applications.

Setting up Internet Access Restriction

The **SET UP NOW** button appears on the right side of your Intelligent Gateway home page in the Access Controls area.



Network at a Glance

Intelligent Gateway 1800
- Software: 3.3.0
- Password: Not set

- Set system password
- Privacy policy

Broadband Link
Connection Speed:
- Incoming: 576 kbps
- Outgoing: 288 kbps

- Monitor your Internet connection
- View summary

Local Network
Computers:
172.16.1.6

- View the local network

Firewall

Firewall
Active

- View firewall settings
- Monitor the firewall

Firewall Monitor
Available!
VIEW NOW

Access Controls

Internet Access Restriction
Installed!
SET UP NOW

- View access controls
- View log

Content Screening
Installed!
SET UP NOW

Upgrade the System

Your system software is current. Check back for future available upgrades.

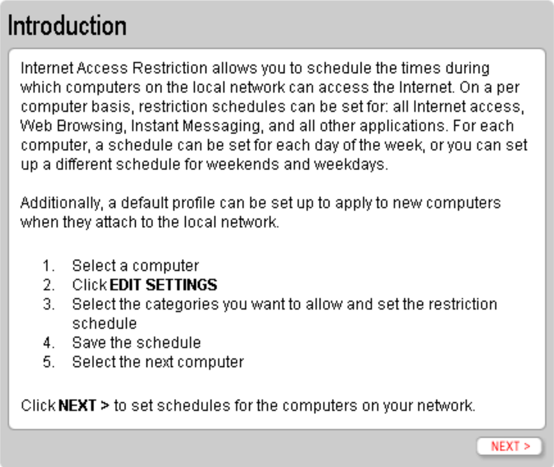
- View available upgrades and options

Set Up

Run the System Setup Wizard.

- Registration info
- Run System Setup Wizard

- To begin configuring the Internet Access Restriction feature, click **SET UP NOW**.
- The Set Up Internet Access Restriction page opens.



Introduction

Internet Access Restriction allows you to schedule the times during which computers on the local network can access the Internet. On a per computer basis, restriction schedules can be set for: all Internet access, Web Browsing, Instant Messaging, and all other applications. For each computer, a schedule can be set for each day of the week, or you can set up a different schedule for weekends and weekdays.

Additionally, a default profile can be set up to apply to new computers when they attach to the local network.

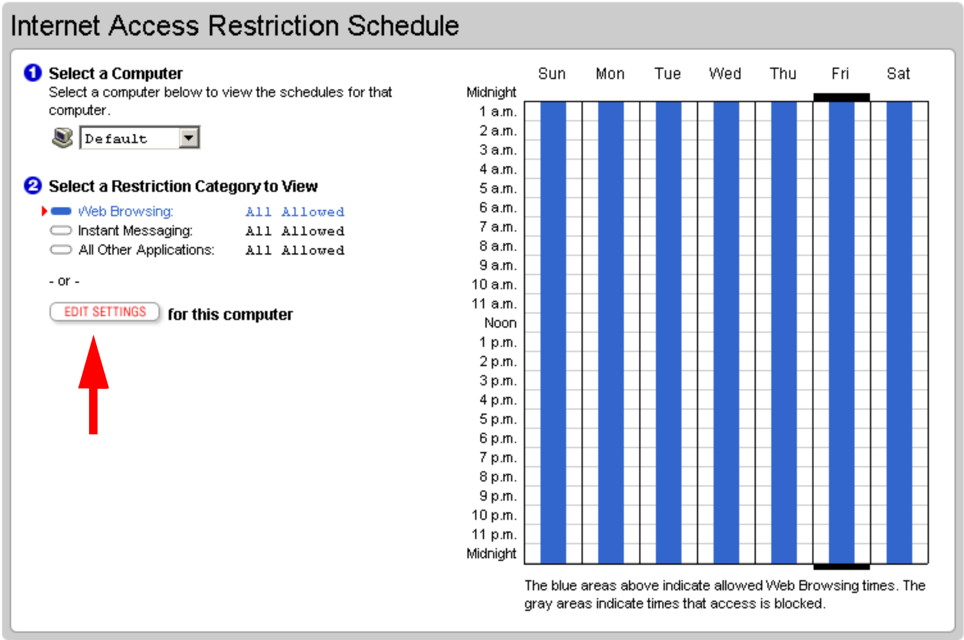
1. Select a computer
2. Click **EDIT SETTINGS**
3. Select the categories you want to allow and set the restriction schedule
4. Save the schedule
5. Select the next computer

Click **NEXT >** to set schedules for the computers on your network.

- Read the Introduction for a summary of Internet Access Restriction features and configuration setup sequence.

- Click **NEXT** to see the Internet Access Restriction Schedule and begin defining schedules for the computers on your network.

Note: *Initially, all computers set up on your local network default to have full access to the Internet.*



Internet Access Restriction Schedule

1 Select a Computer
Select a computer below to view the schedules for that computer.

Default

2 Select a Restriction Category to View

Web Browsing: All Allowed
Instant Messaging: All Allowed
All Other Applications: All Allowed

- or -

EDIT SETTINGS **for this computer**

The blue areas above indicate allowed Web Browsing times. The gray areas indicate times that access is blocked.

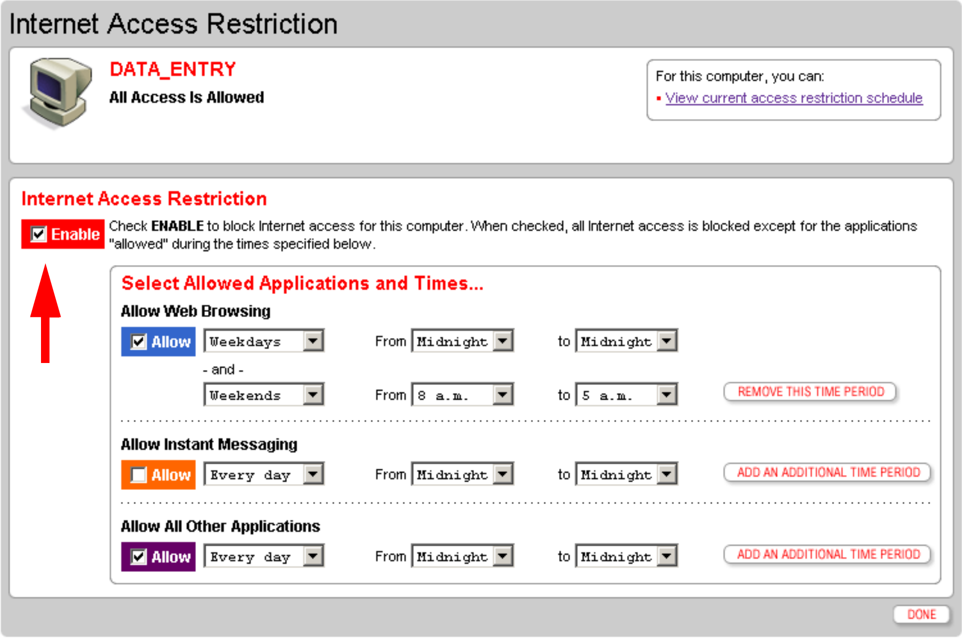
Step 1: Define Internet Access Restriction settings

For each computer on the network, you can block access to all Internet applications or block access to specific types of applications (such as Instant Messaging or Web browsing).

Note: *To secure your Intelligent Gateway settings, be sure to set a system password. The Edit Settings page is protected by the system password. If you have set a system password for your Intelligent Gateway, you are prompted to enter the password before you can edit the settings.*

To add or edit the access control settings for a given computer, click the **EDIT SETTINGS** button on the Internet Access Restriction Schedule page.

The Edit Internet Access Restriction Settings page opens.



Internet Access Restriction

DATA_ENTRY

All Access Is Allowed

For this computer, you can:
- View current access restriction schedule

Internet Access Restriction

☑ Enable Check **ENABLE** to block Internet access for this computer. When checked, all Internet access is blocked except for the applications "allowed" during the times specified below.

Select Allowed Applications and Times...

Allow Web Browsing

☑ Allow Weekdays From Midnight to Midnight

- and -

Weekends From 8 a.m. to 5 a.m. REMOVE THIS TIME PERIOD

Allow Instant Messaging

□ Allow Every day From Midnight to Midnight ADD AN ADDITIONAL TIME PERIOD

Allow All Other Applications

☑ Allow Every day From Midnight to Midnight ADD AN ADDITIONAL TIME PERIOD

DONE

The upper portion of the page displays the summary of restrictions that are applied to the selected computer. The lower portion of the page is used to modify the restriction schedules of each category for this computer.

Step 2: Enable Internet Access Restriction

To begin setting up a schedule of allowed applications (or restrict Internet access altogether) for this computer, you must first enable Internet Access Restriction by clicking the **ENABLE** checkbox in the upper left corner of the Restrict Internet Access area. This action restricts all Internet access, regardless of category, day of the week, and so on. Leaving this box unchecked allows full access to the Internet.

Step 3: Permit and schedule a specific application category

After restricting Internet access, you can permit certain application categories to be accessible either all the time or according to a schedule that you configure.

Internet Access categories

Internet Access categories are predefined groups of Internet applications that can be used to provide flexibility and ease in defining Internet access for computers on your local network. You can also adjust Internet Access schedules, per category, for each day of the week. For example, you can set up a different schedule for Web browsing on weekdays and weekends.

For each computer on your network, you can set Internet Access schedules that allow:

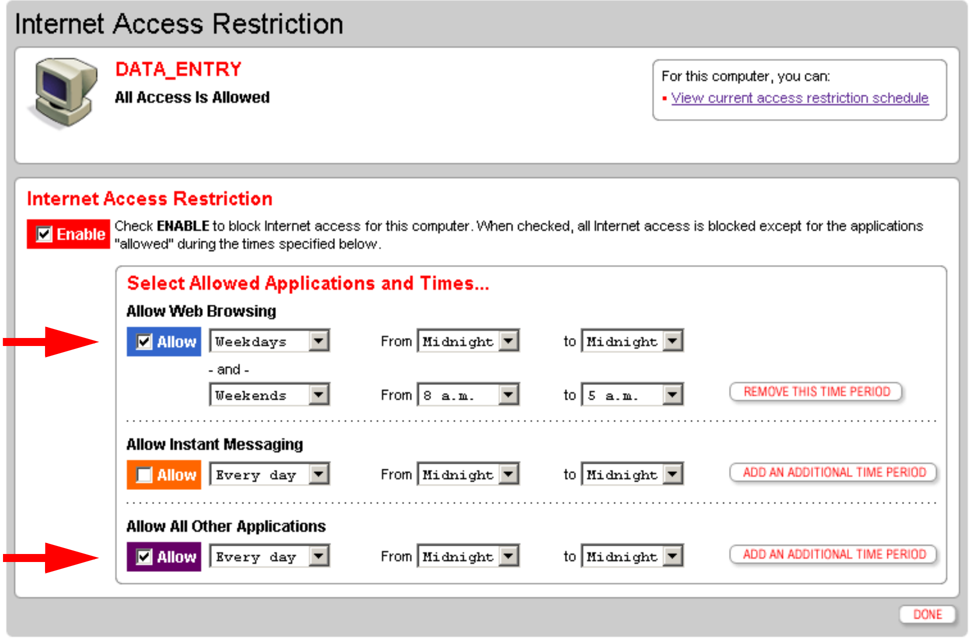
- **Allow Web Browsing** - Choosing the Web Browsing category allows basic Web surfing using an Internet browser, such as Microsoft Internet Explorer™ or Netscape Communicator™. Other applications that require Internet access, such as email services and Internet Messaging, are not available unless allowed under other categories.

- **Allow Instant Messaging** - Choosing the instant messaging category allows access to common instant messaging applications, such as AOL Instant Messenger™, Yahoo Messenger™, and ICQ™. All other Web services are not active, including Web browsing.
- **Allow All Other Applications** - Choosing the All Other Applications category permits all other application types, except Web browsing and Instant Messaging unless allowed under other categories.

Permitting use of a specific application

To permit a specific application category, regardless of the day of the week or time of day, follow these steps:

1. With Internet Access Restriction enabled, click the **ALLOW** checkbox for the application category that you wish to enable. For example to allow Web browsing all day, every day, click the blue Allow checkbox in the Allow Web Browsing area.
2. Click the **DONE** button on the lower right of the screen to ensure that your changes have been saved.



Internet Access Restriction

DATA_ENTRY

All Access Is Allowed

For this computer, you can:
- View current access restriction schedule

Internet Access Restriction

☑ Enable Check **ENABLE** to block Internet access for this computer. When checked, all Internet access is blocked except for the applications "allowed" during the times specified below.

Select Allowed Applications and Times...

Allow Web Browsing

☑ Allow Weekdays From Midnight to Midnight

- and -

Weekends From 8 a.m. to 5 a.m. REMOVE THIS TIME PERIOD

Allow Instant Messaging

☐ Allow Every day From Midnight to Midnight ADD AN ADDITIONAL TIME PERIOD

Allow All Other Applications

☑ Allow Every day From Midnight to Midnight ADD AN ADDITIONAL TIME PERIOD

DONE

Permitting applications only during a specific schedule

To permit a specific application category according to a schedule, follow these steps:

1. With Internet Access Restriction enabled, click the ALLOW checkbox for the application category that you wish to enable.
2. Select a specific day, weekdays, or weekends from the dropdown menu.
3. Specify the From and To times you want the specific category to be allowed. For example, you can choose to allow Web browsing Every day, from 6:00 p.m. until 9:00 p.m.

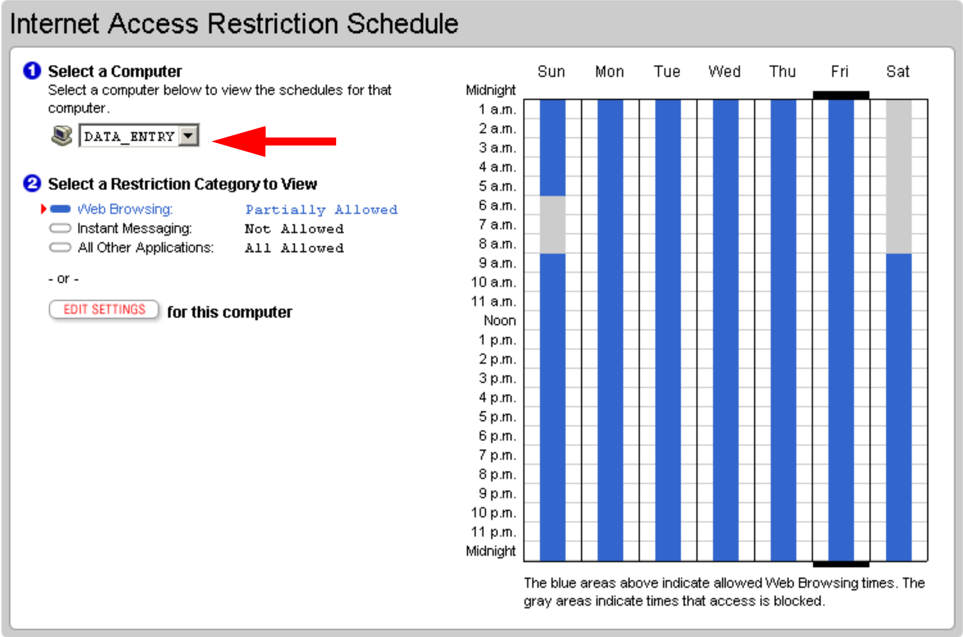
Note: *Schedules that span midnight may produce unexpected results. For example, if you set a schedule for weekends from 8:00 PM to 6:00 AM, the schedule runs from 8:00 PM Saturday night through 6:00 AM Monday morning. It does not include 12:00 AM through 6:00 AM Saturday morning.*

4. To add multiple days and times, click **ADD AN ADDITIONAL TIME PERIOD** and repeat the previous steps.
5. After you are satisfied with the settings you have selected, click the **DONE** button on the lower right of the screen.

Viewing a restriction schedule

To view the restriction schedule for a specific computer, from the Select a Computer dropdown list, select the computer name. The page is automatically updated to display the restriction schedule for the selected computer.

This page displays the restrictions applied to each computer on your network. The page also provides details about the restriction categories that have been assigned and displays a graphical calendar that indicates the time intervals that each category is blocked or allowed.



Internet Access Restriction Schedule

1 Select a Computer

Select a computer below to view the schedules for that computer.

DATA_ENTRY

2 Select a Restriction Category to View

Web Browsing:	Partially Allowed
Instant Messaging:	Not Allowed
All Other Applications:	All Allowed

- or -

EDIT SETTINGS for this computer

The blue areas above indicate allowed Web Browsing times. The gray areas indicate times that access is blocked.

Note: *The Default Settings computer in the dropdown list is a placeholder for any new computers that join the local network. For example, if you buy a new computer or bring a laptop home from work for the first time, when you add this new computer to your local network it automatically acquires the default access configuration you have specified.*

To view the schedule for a different category, click the oval bullet next to the category. The page is automatically updated and a summary of the schedule for the category is displayed.

Each category has one of three designations:

- **All Allowed** - No restrictions exist for this category of applications. This category of applications can access the Internet at any time.
- **Partially Allowed** - The associated category is blocked only for certain time periods. For more detailed information, including time and day that the specified application is partially blocked, click the oval bullet located to the left of the category name. The calendar display at the right of the screen is updated to indicate which time and day of the week the specified application is blocked.
- **Not Allowed** - The associated category is blocked at all times and cannot be accessed from the selected computer.

Content Screening

The Content Screening section of the Access Control application provides the highest level of protection available by:

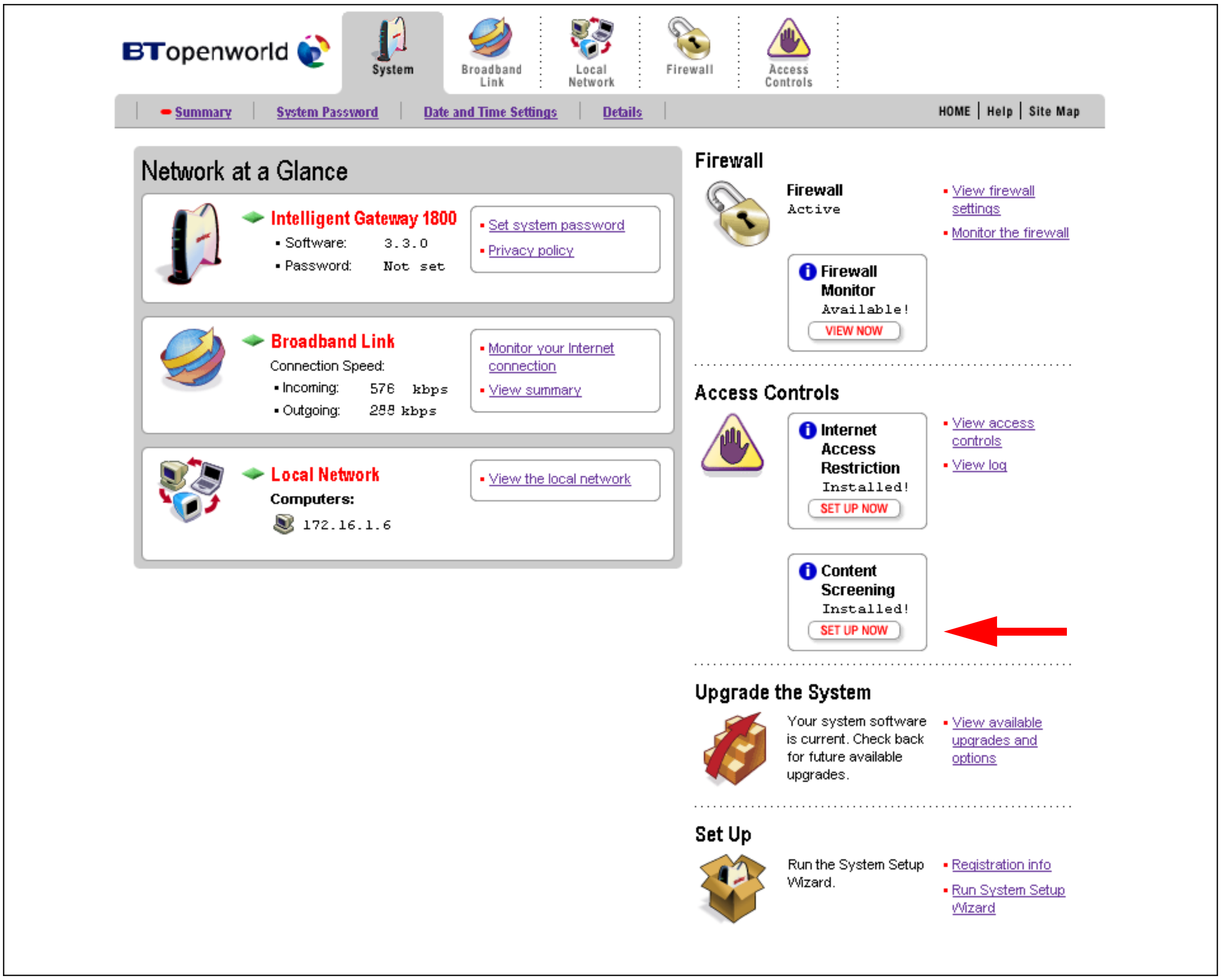
- Providing access to sites that you have defined as approved.
- Blocking or limiting access to specified sites and allowing creation of a list of approved sites for employee browsing.
- Safeguarding your office from Web sites promoting objectionable content.
- Providing continuously updated Web site screening lists so the categories that you guard against always contain the most recent entries.

Each time a Web site is accessed from the specified computer, the Web site address is checked against an online database of harmful and questionable Web site addresses. If the requested Web site falls into a category that is restricted, and that category is indicated to be screened, access to the site is denied and a message is sent to the browser window on the computer informing the user that access for that Web site is blocked.

In addition to Web sites being listed in the database, you can block access to any specific site by manually adding it to the blocked list. Similarly, if you wish to block access to a specific category of content, but would like to allow access to a particular site that would normally be blocked in that category, you can permit access to a specific Web site by adding it to the approved list.

Setting up Content Screening

To configure Content Screening, click the **SET UP NOW** button on the right side of your Intelligent Gateway home page in the Access Controls area.



Network at a Glance

Intelligent Gateway 1800
- Software: 3.3.0
- Password: Not set

- Set system password
- Privacy policy

Broadband Link
Connection Speed:
- Incoming: 576 kbps
- Outgoing: 288 kbps

- Monitor your Internet connection
- View summary

Local Network
Computers:
172.16.1.6

- View the local network

Firewall

Firewall
Active

- View firewall settings
- Monitor the firewall

Firewall Monitor
Available!
VIEW NOW

Access Controls

Internet Access Restriction
Installed!
SET UP NOW

- View access controls
- View log

Content Screening
Installed!
SET UP NOW

Upgrade the System

Your system software is current. Check back for future available upgrades.

- View available upgrades and options

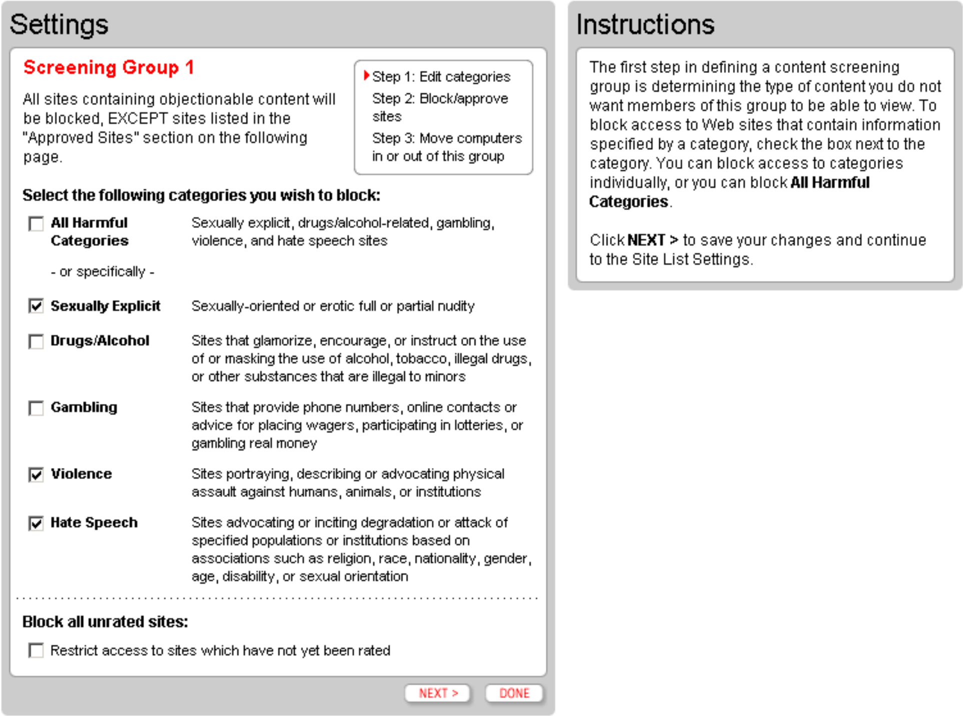
Set Up

Run the System Setup Wizard.

- Registration info
- Run System Setup Wizard

Step 1: Block content categories for this screening group

After initiating the set up for Content Screening, the Block Content Categories for This Screening Group page opens. Use this page to set up the blocked content category for Screening Group 1.



Screening Group 1

All sites containing objectionable content will be blocked, EXCEPT sites listed in the "Approved Sites" section on the following page.

- Step 1: Edit categories
- Step 2: Block/approve sites
- Step 3: Move computers in or out of this group

Select the following categories you wish to block:

□ **All Harmful Categories**	Sexually explicit, drugs/alcohol-related, gambling, violence, and hate speech sites
- or specifically -	
☑ **Sexually Explicit**	Sexually-oriented or erotic full or partial nudity
□ **Drugs/Alcohol**	Sites that glamorize, encourage, or instruct on the use of or masking the use of alcohol, tobacco, illegal drugs, or other substances that are illegal to minors
□ **Gambling**	Sites that provide phone numbers, online contacts or advice for placing wagers, participating in lotteries, or gambling real money
☑ **Violence**	Sites portraying, describing or advocating physical assault against humans, animals, or institutions
☑ **Hate Speech**	Sites advocating or inciting degradation or attack of specified populations or institutions based on associations such as religion, race, nationality, gender, age, disability, or sexual orientation

Block all unrated sites:

□ Restrict access to sites which have not yet been rated

The first step in defining a content screening group is determining the type of content you do not want members of this group to be able to view. To block access to Web sites that contain information specified by a category, check the box next to the category. You can block access to categories individually, or you can block **All Harmful Categories**.

Click **NEXT >** to save your changes and continue to the Site List Settings.

Content categories

To make it easier to block undesirable content, a number of content categories have been developed. Professional researchers working with a third-party maintain a database of Web site addresses that fall under specified content categories. In addition, you can use the blocked list and approved list features of the content screening application to manually block or permit specific sites that may or may not fall under the categories outlined below.

Any online content that contains more than 3 instances in 100 messages or any easily accessible pages with graphics, text or audio that fall within the definition of the categories shown below are considered sufficient to place the source site in that category. Internet sites that contain information or software programs designed to hack into filtering software are added to the database in *all* categories.

Note: *BT Openworld has used what we believe to be reasonable means to identify and categorize Web sites, but cannot guarantee the accuracy or completeness of our screens and assumes no responsibility for errors or omissions.*

The following types of content are filtered by each category:

- Sexually Explicit

Note: *Sites regarding sexual health, breast cancer, or sexually transmitted diseases (except in graphic examples) are not blocked. In addition, sites containing nudity or partial nudity of a non-prurient nature are not blocked (for example, Web sites for publications such as National Geographic or Smithsonian magazine or sites hosted by museums such as the Guggenheim, the Louvre, or the Museum of Modern Art.)*

- Drugs/Alcohol

Note: *Sites discussing medicinal drug use, industrial hemp use, or public debate on the issue of legalizing certain drugs are not blocked, nor are sites sponsored by a public or private agency that provides educational information on drug use.*

- Gambling
- Hate Speech

Note: *Sites that contain news, historical, or press incidents are not blocked.*

- Violence

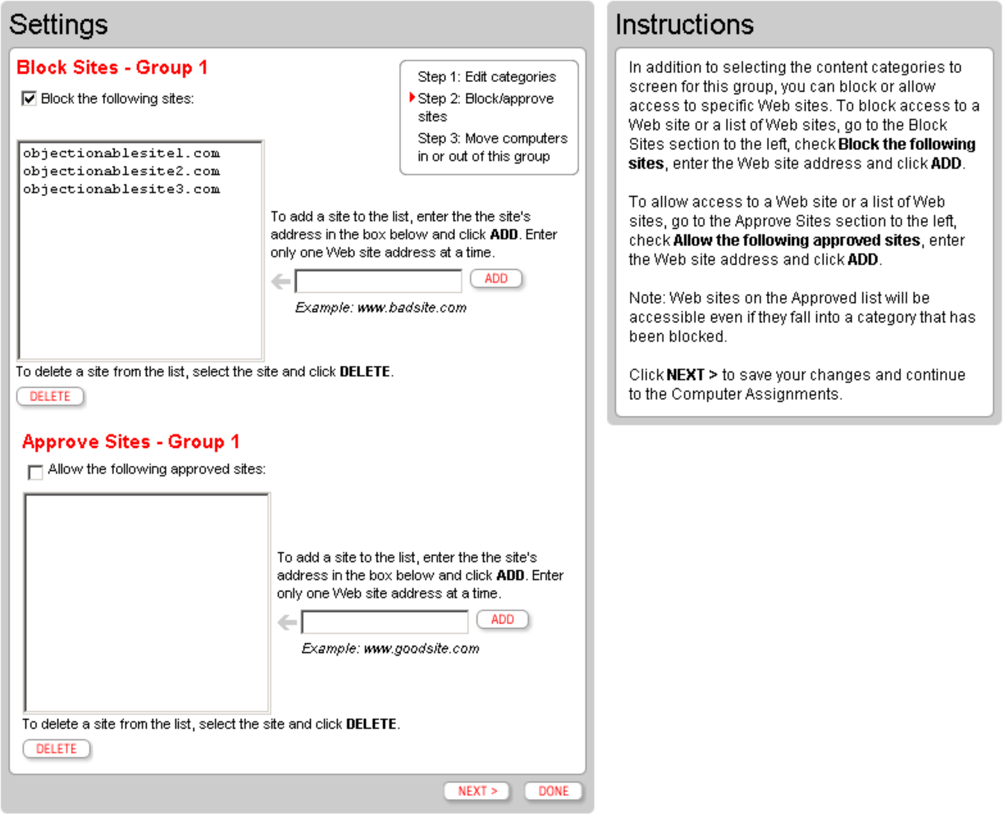
Note: *Sites that contain news, historical, or press incidents are not blocked.*

From the Category Settings page, you can choose to block all of the content categories listed or select individual categories. Place a check mark in the box next to each category you want to block. Computers in this screening group will not have access to the specified content of the selected categories.

Click **NEXT** to save your category choices and proceed to the second step. Click **DONE** to return to the home page.

Step 2: Block and approve sites for this screening group

After selecting the categories of content to be blocked, the Site List Settings page opens. This page allows you to block or approve up to 128 specific sites. Any sites added to the Block Sites lists are blocked for all computers assigned to the screening group. Similarly, regardless of whether or not they appear in one of the selected category lists, sites added to the Approved Sites list are accessible and override the blocked category setting if that specific Web site falls into the blocked category.



Settings

Block Sites - Group 1

☑ Block the following sites:

objectionablesite1.com
objectionablesite2.com
objectionablesite3.com

Step 1: Edit categories
Step 2: Block/approve sites
Step 3: Move computers in or out of this group

To add a site to the list, enter the the site's address in the box below and click **ADD**. Enter only one Web site address at a time.

Example: www.badsite.com

To delete a site from the list, select the site and click **DELETE**.

Approve Sites - Group 1

☐ Allow the following approved sites:

To add a site to the list, enter the the site's address in the box below and click **ADD**. Enter only one Web site address at a time.

Example: www.goodsite.com

To delete a site from the list, select the site and click **DELETE**.

Instructions

In addition to selecting the content categories to screen for this group, you can block or allow access to specific Web sites. To block access to a Web site or a list of Web sites, go to the Block Sites section to the left, check **Block the following sites**, enter the Web site address and click **ADD**.

To allow access to a Web site or a list of Web sites, go to the Approve Sites section to the left, check **Allow the following approved sites**, enter the Web site address and click **ADD**.

Note: Web sites on the Approved list will be accessible even if they fall into a category that has been blocked.

Click **NEXT >** to save your changes and continue to the Computer Assignments.

Adding sites

To add a site to either the blocked or approved list, enter the address of the Web site in the Block Sites box or the Approve Sites box and click **ADD**.

Note: *When adding a specific site to either list, you can exclude the http://www portion of the address. For example, if you are adding http://www.abc.com to either list, you need only enter abc.com.*

Removing sites

To remove a Web site from one of the lists, highlight the site and click **DELETE**.

Allowing blocked sites

To stop blocking all of the sites listed in the Block Sites list (in other words, allow all sites), remove the check from the Block sites listed checkbox.

Blocking approved sites

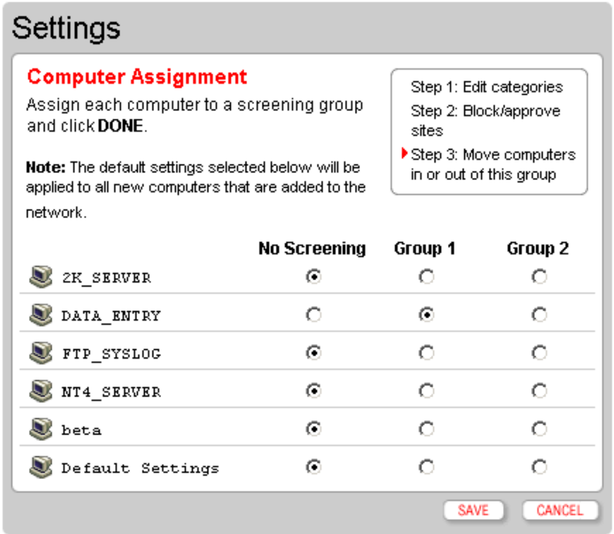
To stop permitting access to the Approve Sites list, remove the check from the Always allow sites listed checkbox.

Click **NEXT** to save all of the blocked and approved Web sites you have entered and proceed to the third step. Click **DONE** to return to the home page.

Step 3: Assign computers to screening groups

After setting up the content categories and sites that are blocked and approved for a screening group, you can assign computers to that screening group.

To set up computer assignments, use the Settings area of the Assign Computers to Screening Groups page.



Settings

Computer Assignment

Assign each computer to a screening group and click **DONE**.

Note: The default settings selected below will be applied to all new computers that are added to the network.

Step 1: Edit categories
Step 2: Block/approve sites
Step 3: Move computers in or out of this group

	No Screening	Group 1	Group 2
2K_SERVER	●	○	○
DATA_ENTRY	○	●	○
FTP_SYSLOG	●	○	○
NT4_SERVER	●	○	○
beta	●	○	○
Default Settings	●	○	○

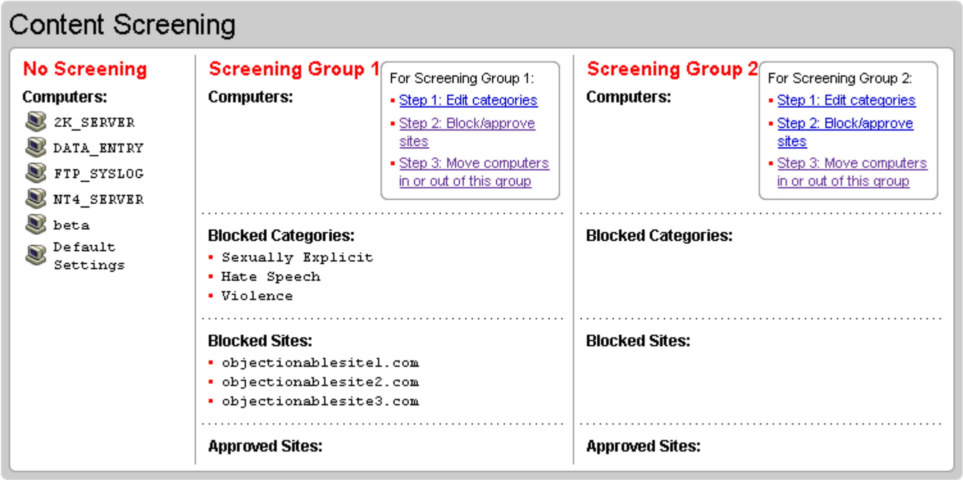
To assign a computer to a particular group, click the radio button to the right of the computer in the column of the desired group.

The Default Settings computer is a placeholder for any new computers that join the local network. For example, if you buy a new computer or bring a laptop home from work for the first time, when you add this new computer to your local network it automatically acquires the default access configuration you have specified. Initially, you should use the maximum amount of screening as the default and then reduce the level of blocked content as needed.

Click **SAVE** to record your changes.

Viewing Content Screening settings

Use the View Content Screening Settings page to view the current content screening settings for your network.



Content Screening

No Screening

Computers:
- 2K_SERVER
- DATA_ENTRY
- FTP_SYSLOG
- NT4_SERVER
- beta
- Default Settings

Screening Group 1

Computers:

For Screening Group 1:
- Step 1: Edit categories
- Step 2: Block/approve sites
- Step 3: Move computers in or out of this group

Blocked Categories:
- Sexually Explicit
- Hate Speech
- Violence

Blocked Sites:
- objectionablesite1.com
- objectionablesite2.com
- objectionablesite3.com

Approved Sites:

Screening Group 2

Computers:

For Screening Group 2:
- Step 1: Edit categories
- Step 2: Block/approve sites
- Step 3: Move computers in or out of this group

Blocked Categories:

Blocked Sites:

Approved Sites:

The Content Screening Summary Page displays:

- The computer assigned to each group.
- The categories of blocked content for each group.
- Additional sites that are blocked for viewing.
- Additional sites that are approved for viewing.

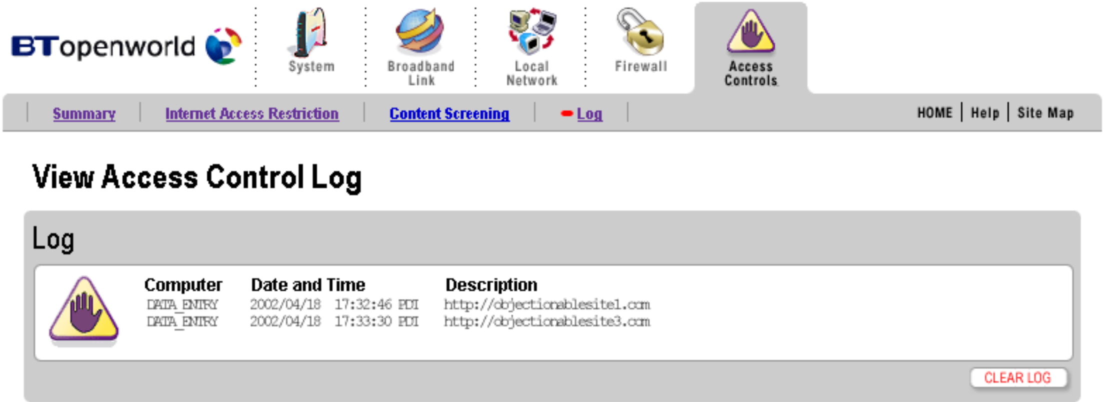
Access Controls log

Use the Access Controls log to view a log of specific sites and applications that have been blocked for a particular computer. For example, assume www.abc.com is in the content screening database to be blocked for violent content. Violent content is blocked in screening Group 1. Each time an employee from this group tries to access www.abc.com, an entry is added to the log. Similarly, if a certain application type (such as instant messaging or chat) is restricted through the use of the Internet Access Restriction application and someone attempts to access the Internet using that application, the activity is recorded in the log.

To view the Access Controls log, follow these steps:

1. Launch a browser window and type `officeportal` to access the Intelligent Gateway Home page of the user interface.
2. On the main navigation bar at the top of your browser window, click the **Access Controls** tab.

3. Click **LOG** to view the Access Controls log.



View Access Control Log

Log

Computer	Date and Time	Description
DATA_ENTRY	2002/04/18 17:32:46 PDT	http://objectionablesite1.com
DATA_ENTRY	2002/04/18 17:33:30 PDT	http://objectionablesite3.com

To clear the log, click the **CLEAR LOG** button, located in the corners of the right side of the page.

Sharing Files and Printers

PC/network configuration for file sharing

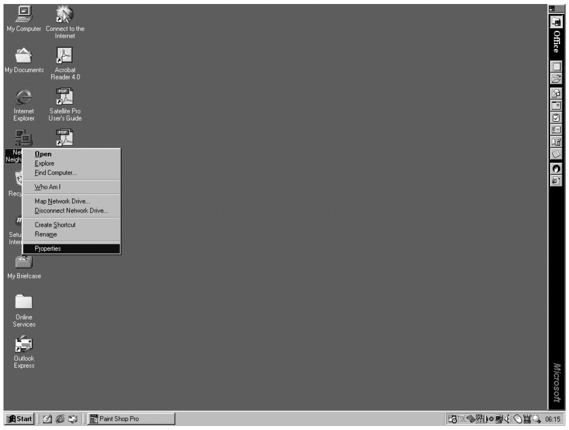
This chapter describes how to set up a network for file / printer sharing between PCs. If wireless networking is being added to an existing network (especially where network login is required) please check with your network administrator / consultant before making any changes.

Windows 95, 98, 98 SE operating systems

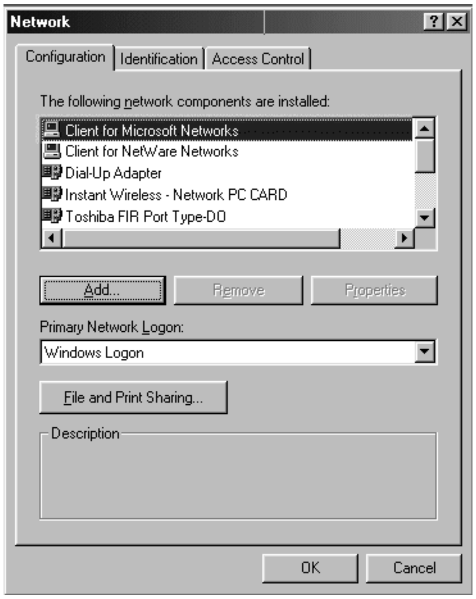
Adding PCs to your network

After you have set up your network, you now need to add each PC to the network.

1. Right-click **Network Neighborhood** and select **Properties**.



2. The Network Properties screen opens. Select **Client for Microsoft Networks** and then click the **Properties** button.

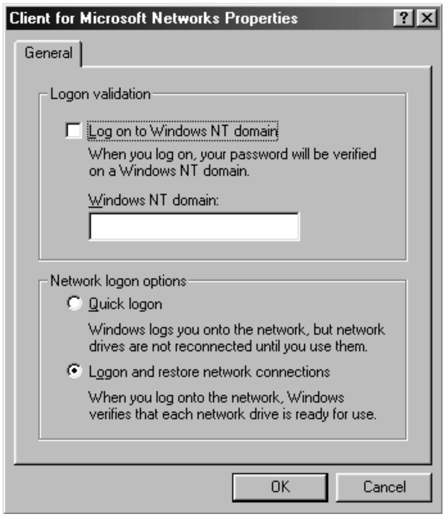


The following network components are installed:

- Client for Microsoft Networks
- Client for NetWare Networks
- Dial-Up Adapter
- Instant Wireless - Network PC CARD
- Toshiba FIR Port Type-DO

Primary Network Logon: Windows Logon

3. Ensure that the Logon validation fields are empty, and that the **Logon and restore network connections** radio button is selected. Click **OK**.



Logon validation

□ Log on to Windows NT domain

When you log on, your password will be verified on a Windows NT domain.

Windows NT domain:

Network logon options

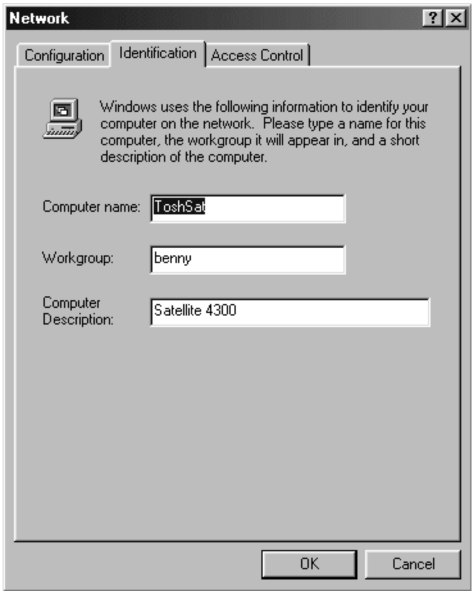
○ Quick logon

Windows logs you onto the network, but network drives are not reconnected until you use them.

● Logon and restore network connections

When you log onto the network, Windows verifies that each network drive is ready for use.

4. Click the Identification tab.
In the Computer name field, enter a name for your computer. In the Workgroup field, enter a workgroup name. ***Do NOT click OK.***



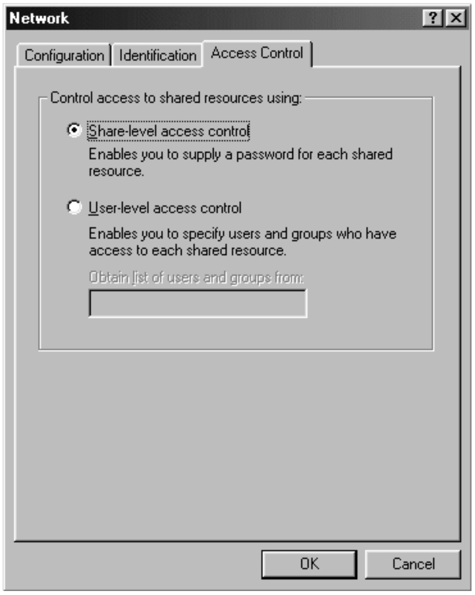
Windows uses the following information to identify your computer on the network. Please type a name for this computer, the workgroup it will appear in, and a short description of the computer.

Computer name: ToshSat

Workgroup: benny

Computer Description: Satellite 4300

5. Click the **Access Control** tab.
In the **Control access to shared resources using** field, click the **Share-level access control** radio button. ***Do NOT click OK.***



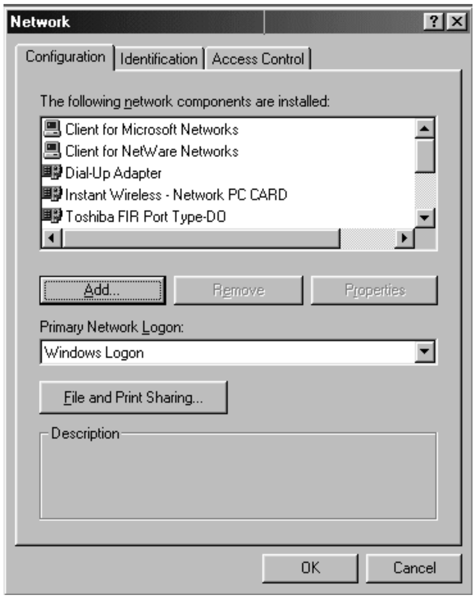
Control access to shared resources using:

● Share-level access control
Enables you to supply a password for each shared resource.

○ User-level access control
Enables you to specify users and groups who have access to each shared resource.

Obtain list of users and groups from:

6. Click the **Configuration** tab.
   In the **Primary Network Logon** field, ensure that **Windows Logon** is selected in the pull-down. Click the **File and Print Sharing** button.

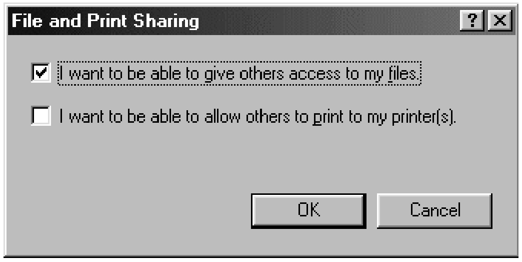


The following network components are installed:

- Client for Microsoft Networks
- Client for NetWare Networks
- Dial-Up Adapter
- Instant Wireless - Network PC CARD
- Toshiba FIR Port Type-DO

Primary Network Logon: Windows Logon

7. Check the **I want to be able to give others access to my files** checkbox and click **OK**.

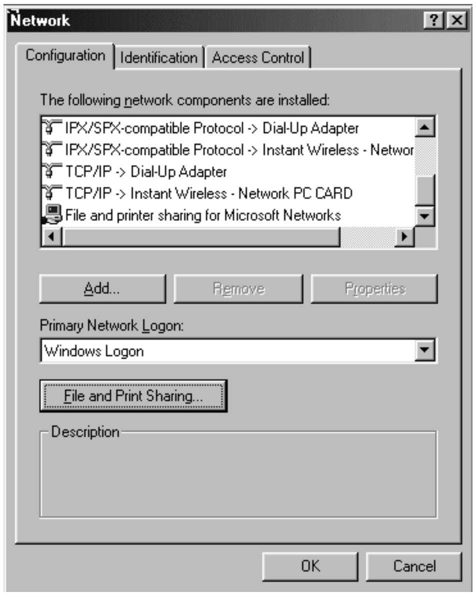


☑ I want to be able to give others access to my files.

☐ I want to be able to allow others to print to my printer(s).

8. File and print sharing will now appear in your network components. Click **OK** for Windows to update your settings.

9. Restart your PC when prompted.



The following network components are installed:

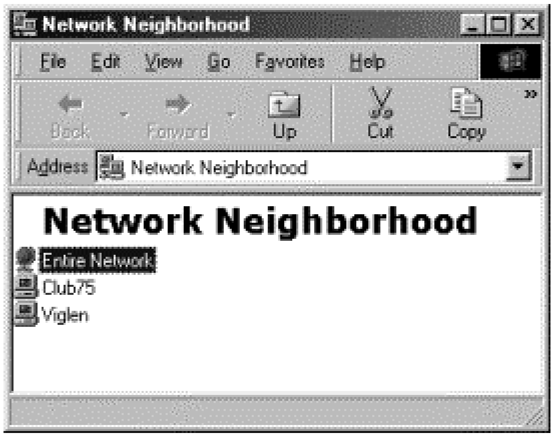
- IPX/SPX-compatible Protocol -> Dial-Up Adapter
- IPX/SPX-compatible Protocol -> Instant Wireless - Networ
- TCP/IP -> Dial-Up Adapter
- TCP/IP -> Instant Wireless - Network PC CARD
- File and printer sharing for Microsoft Networks

Primary Network Logon: Windows Logon

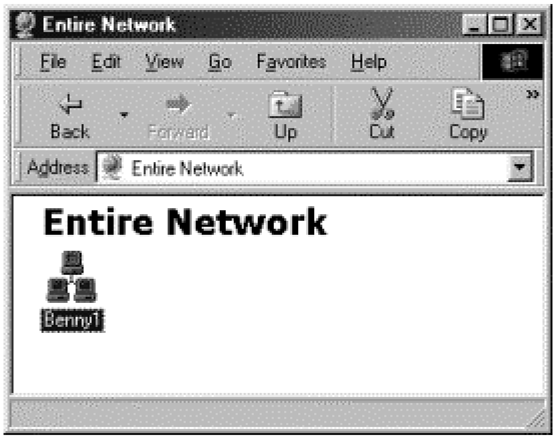
Accessing PCs on your network

1. After you have configured file sharing on your PCs, double-click the **Network Neighborhood** icon to verify that you can see them.

2. In Network Neighborhood, double-click **Entire Network**.

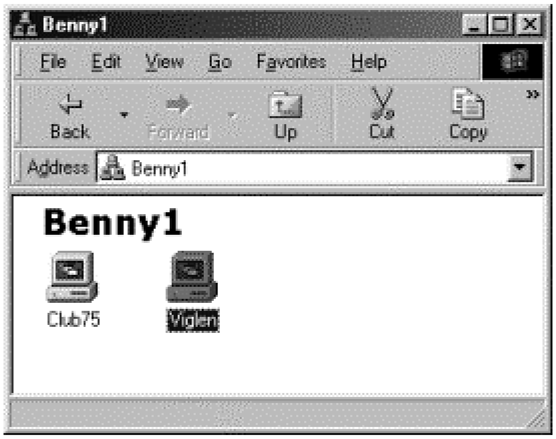


3. In Entire Network, your network name should appear as an icon. Double-click the **icon**.



4. The PCs on your network will be displayed as shown in the screen capture. When file sharing is set up, you will be able to browse the available content of these PCs.

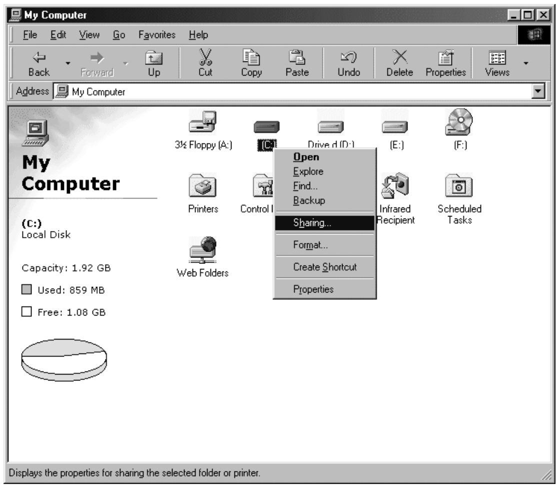
Note: *If you have just added a new PC to the network you may need to select View>Refresh before this will be shown as part of the network.*



Sharing your files

After you have configured file and print sharing, you can choose a drive or folder to share with the other users on your network.

1. Open **My Computer**. Locate your chosen drive or folder and right click it, then click **Sharing**.



My Computer

(C:)
Local Disk

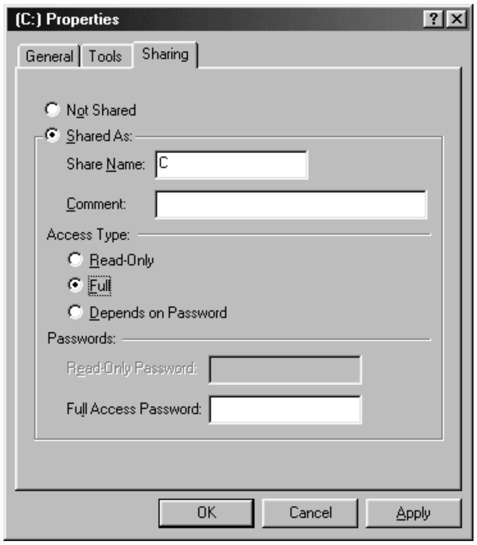
Capacity: 1.92 GB

□ Used: 859 MB

□ Free: 1.08 GB

Displays the properties for sharing the selected folder or printer.

2. In the Sharing tab, click the **Shared As** radio button. In the **Shared Name** field, enter a share name (or accept the default). In the **Access Type** field, click the radio button next to your access preference (Read-Only, Full, or Depends on Password). In the Password field, enter a password if you wish to limit user access, or leave the Password field blank for no password required. Click **Apply** and then **OK** to exit.



○ Not Shared

● Shared As:

Share Name: C

Comment:

Access Type:

○ Read-Only

● Full

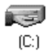
○ Depends on Password

Passwords:

Read-Only Password:

Full Access Password:

3. Your chosen drive or folder will now have the sharing (hand) symbol displayed and will be accessible by others on the network according to the user rights you have set.

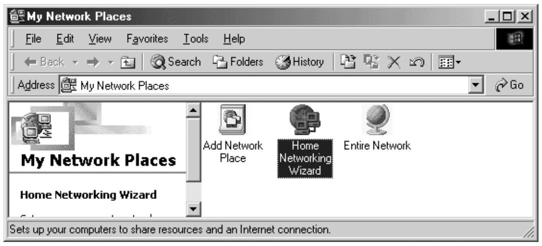


Windows ME operating systems

Adding PCs to your network

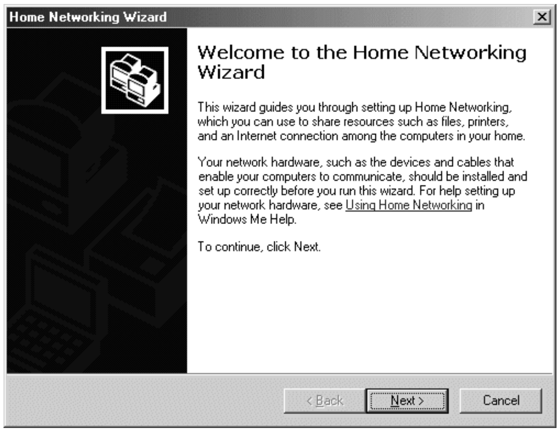
1. Double-click the **My Network Places** icon to open the My Network Places window.

2. Double-click **Home Networking Wizard**.



Sets up your computers to share resources and an Internet connection.

3. When the Wizard opens, click **Next** to continue.



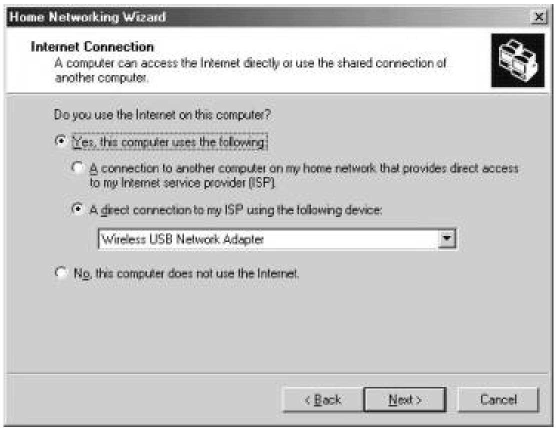
Welcome to the Home Networking Wizard

This wizard guides you through setting up Home Networking, which you can use to share resources such as files, printers, and an Internet connection among the computers in your home.

Your network hardware, such as the devices and cables that enable your computers to communicate, should be installed and set up correctly before you run this wizard. For help setting up your network hardware, see Using Home Networking in Windows Me Help.

To continue, click Next.

4. Select the **Yes, this computer uses the following:** radio button then select the **A direct connection to my ISP using the following device** radio button. Click **Next**.



Internet Connection
A computer can access the Internet directly or use the shared connection of another computer.

Do you use the Internet on this computer?

● Yes, this computer uses the following:

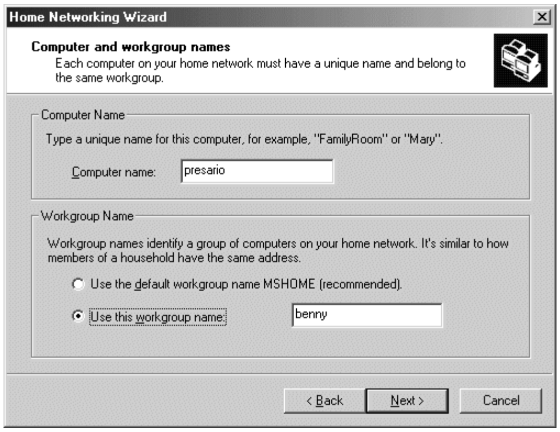
○ A connection to another computer on my home network that provides direct access to my Internet service provider (ISP).

● A direct connection to my ISP using the following device:

Wireless USB Network Adapter

○ No, this computer does not use the Internet.

5. In the **Computer name** field, enter a suitable name for your computer. In the **Workgroup Name** field, select the **Use the Workgroup name** radio button and enter the name of your workgroup (all PCs on your network must have the same workgroup name). Click **Next** to continue.

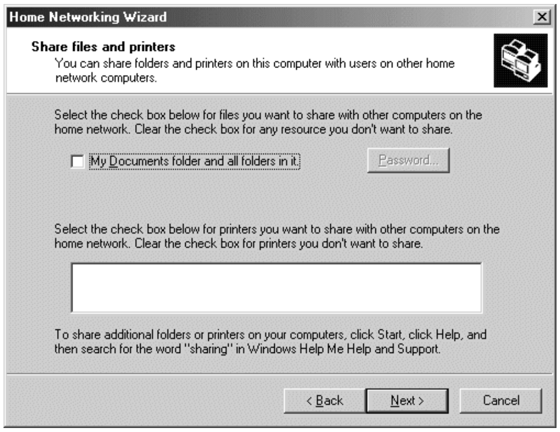


Computer and workgroup names
Each computer on your home network must have a unique name and belong to the same workgroup.

Computer Name
Type a unique name for this computer, for example, "FamilyRoom" or "Mary".
Computer name: presario

Workgroup Name
Workgroup names identify a group of computers on your home network. It's similar to how members of a household have the same address.
○ Use the default workgroup name MSHOME (recommended).
● Use this workgroup name: benny

6. Leave the **Share files and printers** screen blank and click **Next**.



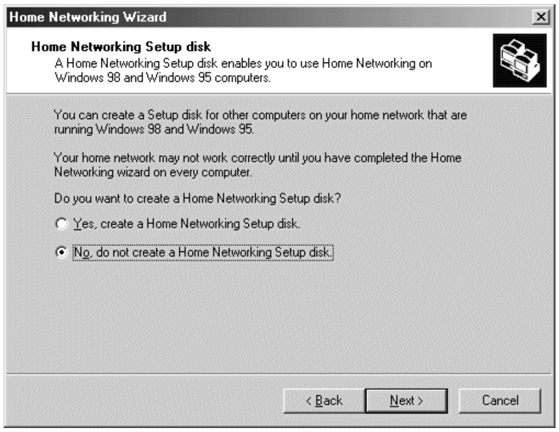
Share files and printers
You can share folders and printers on this computer with users on other home network computers.

Select the check box below for files you want to share with other computers on the home network. Clear the check box for any resource you don't want to share.
□ My Documents folder and all folders in it.

Select the check box below for printers you want to share with other computers on the home network. Clear the check box for printers you don't want to share.

To share additional folders or printers on your computers, click Start, click Help, and then search for the word "sharing" in Windows Help Me Help and Support.

7. Select the **No, do not create a network disk** radio button and **Next** to continue.



Home Networking Setup disk
A Home Networking Setup disk enables you to use Home Networking on Windows 98 and Windows 95 computers.

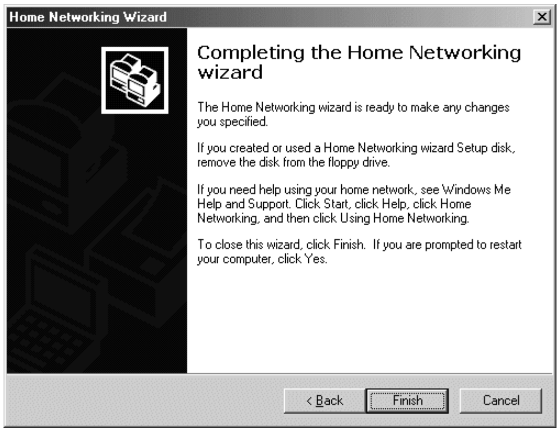
You can create a Setup disk for other computers on your home network that are running Windows 98 and Windows 95.

Your home network may not work correctly until you have completed the Home Networking wizard on every computer.

Do you want to create a Home Networking Setup disk?
○ Yes, create a Home Networking Setup disk.
● No, do not create a Home Networking Setup disk.

8. Click **Finish** to complete your network setup.

9. Restart your PC when prompted.



Completing the Home Networking wizard

The Home Networking wizard is ready to make any changes you specified.

If you created or used a Home Networking wizard Setup disk, remove the disk from the floppy drive.

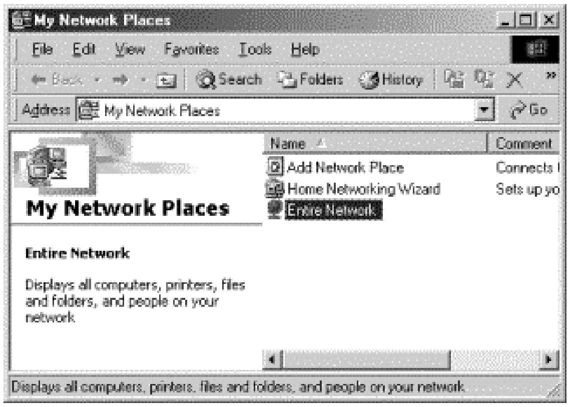
If you need help using your home network, see Windows Me Help and Support. Click Start, click Help, click Home Networking, and then click Using Home Networking.

To close this wizard, click Finish. If you are prompted to restart your computer, click Yes.

Accessing PCs on your network

1. To check that your are connected to the other PCs on your network, double-click the **My Network Places** icon.

2. Double-click **Entire Network**.

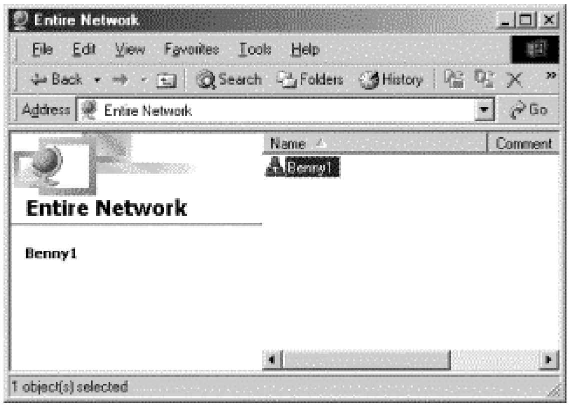


Entire Network

Displays all computers, printers, files and folders, and people on your network

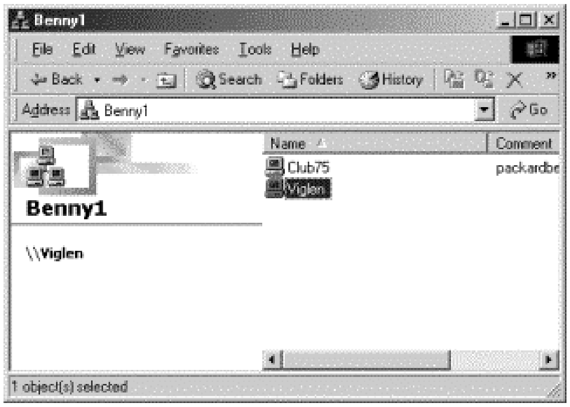
Displays all computers, printers, files and folders, and people on your network

3. An icon will be displayed with your network name. Double-click this icon.



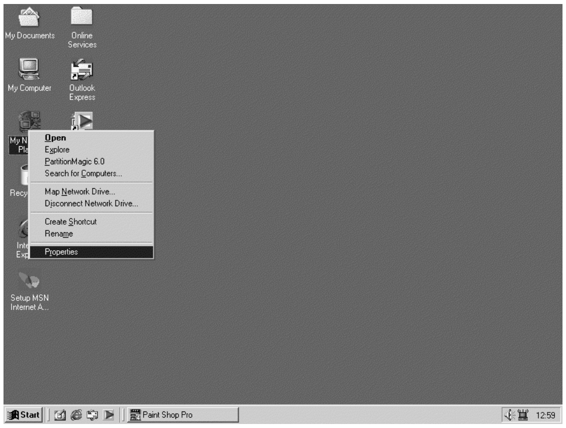
4. The PCs on your network will be displayed. When file sharing is enabled, you can browse the available content of these PCs.

Note: *If you have just added a new PC to the network, you may need to select View>Refresh before this will be shown as part of the network.*

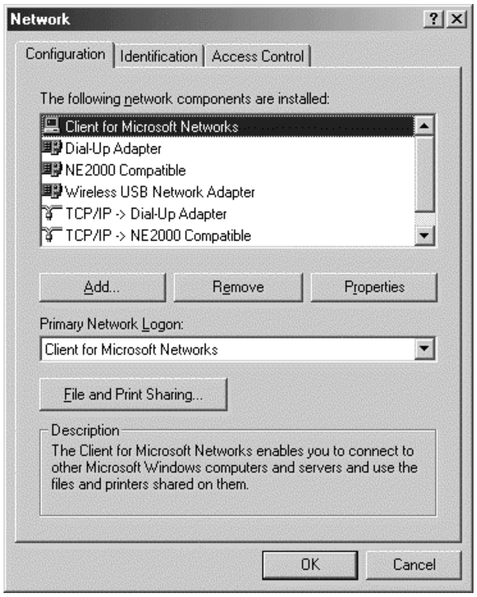


Sharing your files

1. Right-click **My Network Places** and click **Properties**.



2. In the Configuration tab, click the **File and Print Sharing** button.



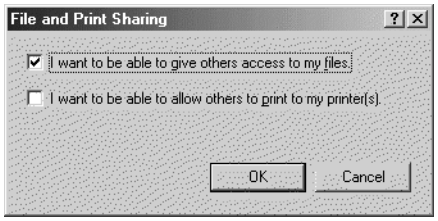
The following network components are installed:

Client for Microsoft Networks
Dial-Up Adapter
NE2000 Compatible
Wireless USB Network Adapter
TCP/IP -> Dial-Up Adapter
TCP/IP -> NE2000 Compatible

Primary Network Logon:
Client for Microsoft Networks

Description
The Client for Microsoft Networks enables you to connect to other Microsoft Windows computers and servers and use the files and printers shared on them.

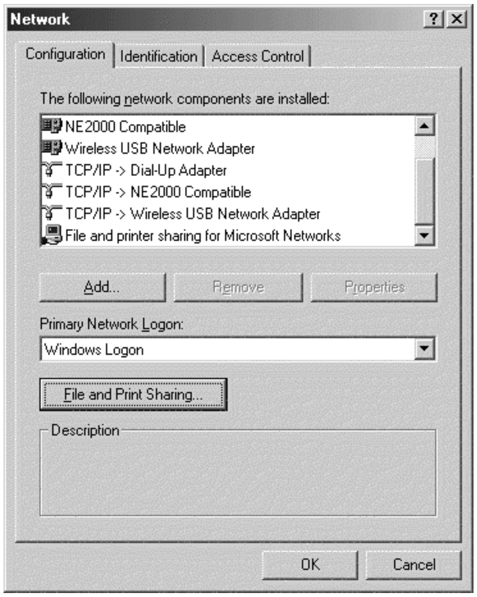
3. Select the **I want to be able to give others access to my files** radio button and click **OK**.



☑ I want to be able to give others access to my files.

☐ I want to be able to allow others to print to my printer(s).

4. File and printer sharing will now appear in your network components list. Click **OK** and restart the PC when prompted.

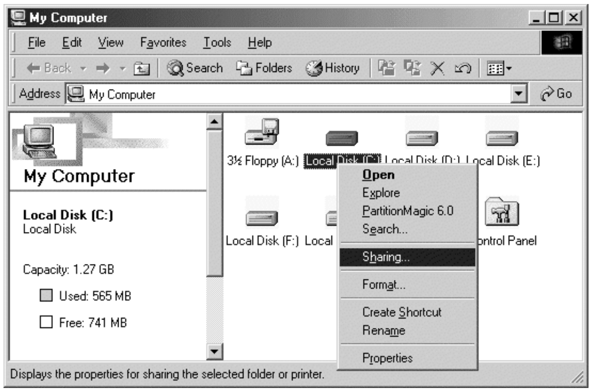


The following network components are installed:

- NE2000 Compatible
- Wireless USB Network Adapter
- TCP/IP -> Dial-Up Adapter
- TCP/IP -> NE2000 Compatible
- TCP/IP -> Wireless USB Network Adapter
- File and printer sharing for Microsoft Networks

Primary Network Logon: Windows Logon

5. When your PC has restarted, open **My Computer** and locate the drive or folder you wish to share. Right click this drive/folder and click **Sharing**.



Local Disk (C:)
Local Disk

Capacity: 1.27 GB

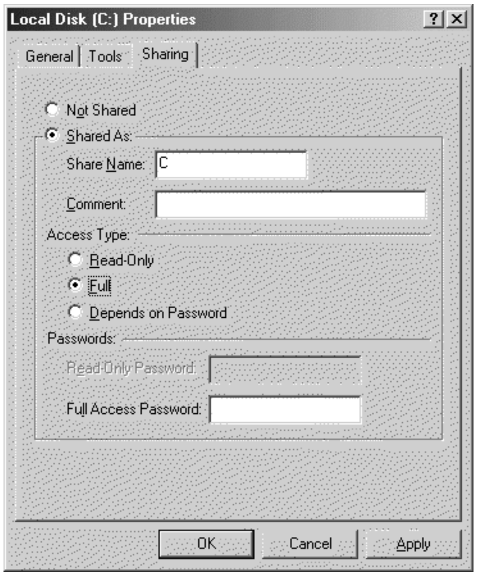
☐ Used: 565 MB

☐ Free: 741 MB

Displays the properties for sharing the selected folder or printer.

6. Select the **Shared As** radio button. In the **Share Name** field, enter a suitable share name (or accept the default). In the **Access Type** field, click the radio button next to your access preference (Read-Only, Full, or Depends on Password). In the Password field, enter a password if you wish to limit user access, or leave the Password field blank for no password required. Click **Apply** and then **OK** to exit.

   Your drive/folder will now be shared and display the Shared (hand) symbol:



○ Not Shared
● Shared As:
Share Name: C
Comment:
Access Type:
○ Read-Only
● Full
○ Depends on Password
Passwords:
Read-Only Password:
Full Access Password:

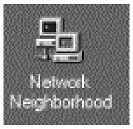
Windows NT operating systems

Adding PCs to your network

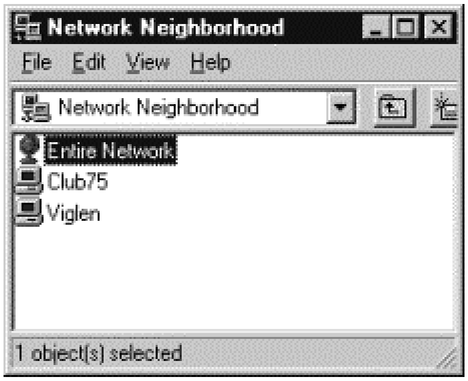
Please note that creating a network in Windows NT is covered in the documentation that came with your Windows NT system, in the network adapter installation section.

Accessing PCs on your network

1. To check that your are connected to the other PCs on your network, double-click the **Network Neighborhood** icon.



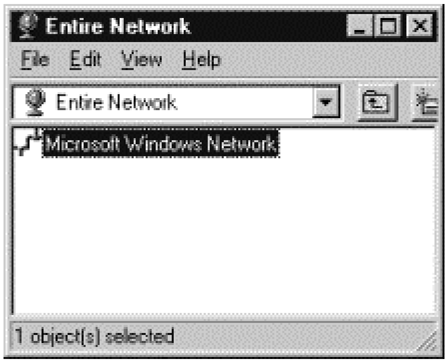
2. Double-click **Entire Network**.



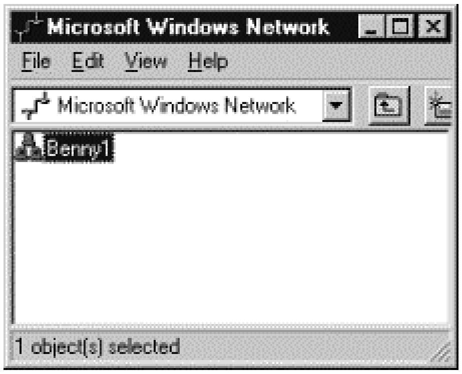
Entire Network
Club75
Viglen

1 object(s) selected

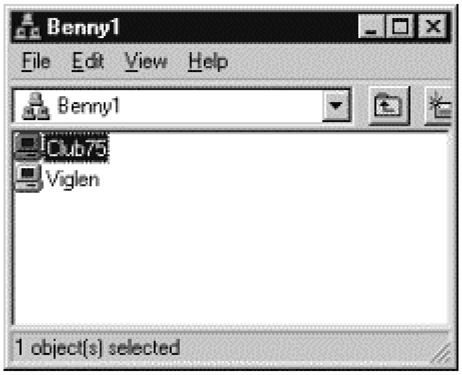
3. Double-click **Microsoft Windows Network**.



4. An icon should be present with your network name. Double-click the icon.



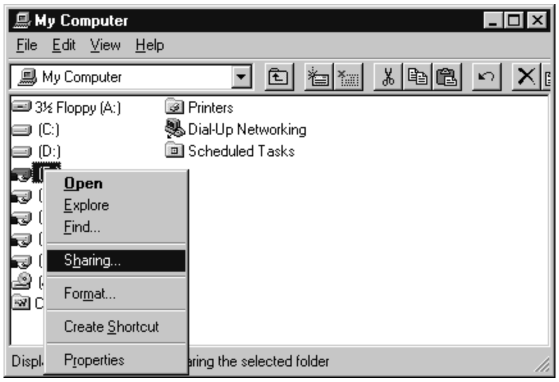
5. The PCs that are in your network will be displayed. When file sharing is set up, you will be able to browse the available content of these PCs.



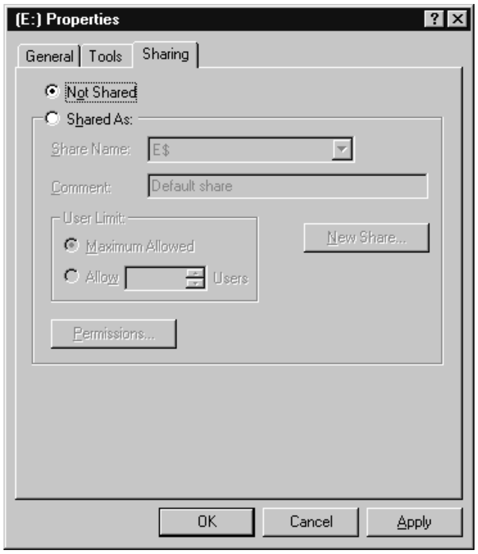
Sharing your files

In Windows NT, file sharing is automatically set up when networking is configured; however, automatic access permissions are set. The following instructions describe how to remove default sharing permissions and customize your permissions.

1. Double-click **My Computer**. For each drive that has the Sharing (hand) symbol, right click that drive and click **Sharing**.

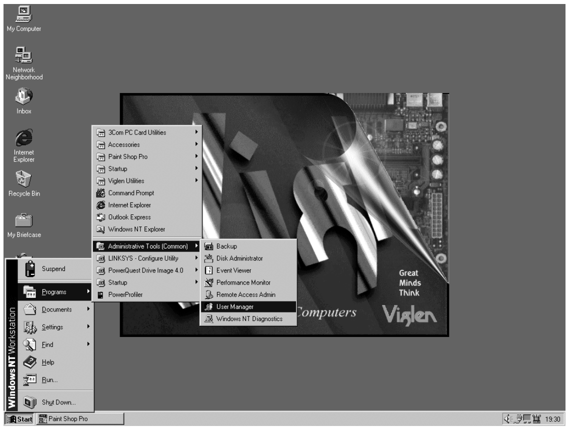


2. In the **Sharing** tab, select the **Not Shared** radio button and click **Apply**. Click **OK** to exit.

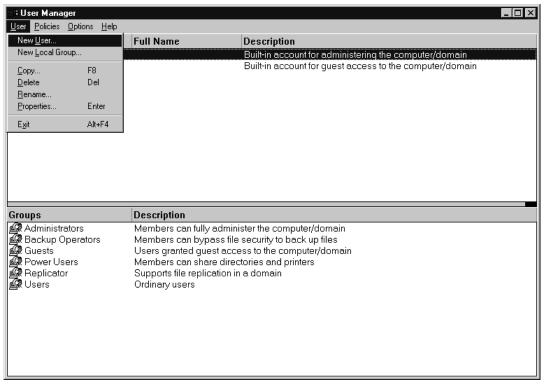


● Not Shared
○ Shared As:
Share Name: E$
Comment: Default share
User Limit:
● Maximum Allowed
○ Allow Users

3. You can now add the other computers you wish to share to your User Group. From the Start menu, select **Programs > Administrative Tools > User Manager**.



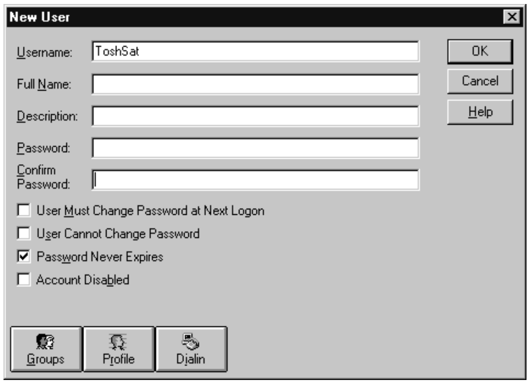
4. In User Manager, click **User** and then **New User**.



Full Name	Description
	Built-in account for administering the computer/domain
	Built-in account for guest access to the computer/domain

Groups	Description
Administrators	Members can fully administer the computer/domain
Backup Operators	Members can bypass file security to back up files
Guests	Users granted guest access to the computer/domain
Power Users	Members can share directories and printers
Replicator	Supports file replication in a domain
Users	Ordinary users

5. In the **Username** field, enter the computer name. This name must be identical to the one you entered in Network Properties. In the **Password** field, enter a password. To make it easy to remember the password, you can use the same password with which the PC logs on to the network. Alternatively, you can leave the **Password** field blank so that no password is required to access folders. If you set up a password, you can set different account options by checking the **User Must Change Password at Next Logon**, **User Cannot Change Password**, or **Password Never Expires** checkboxes. After your choices are entered, click **OK**.



Username: ToshSat

Full Name:

Description:

Password:

Confirm Password:

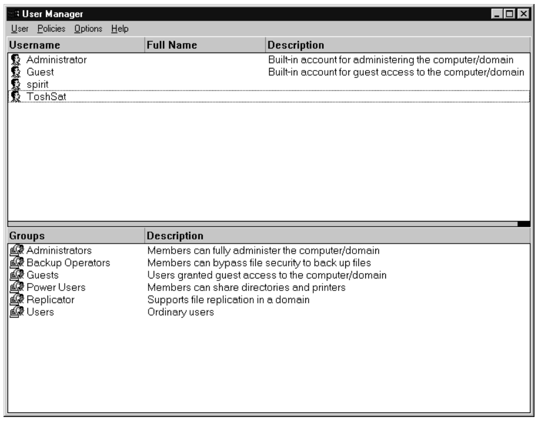
☐ User Must Change Password at Next Logon

☐ User Cannot Change Password

☑ Password Never Expires

☐ Account Disabled

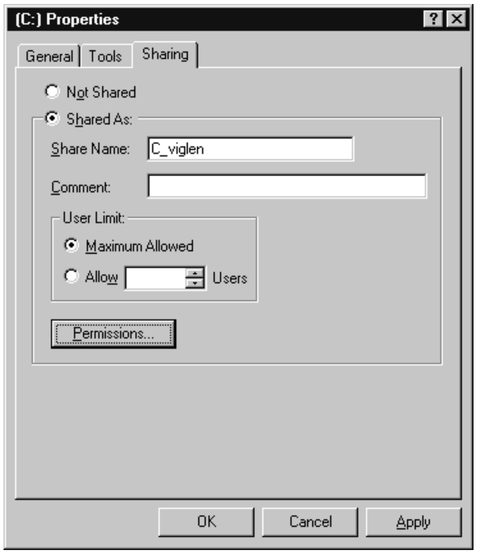
6. Your PC will now appear in User Manager. Close the window.



Username	Full Name	Description
Administrator		Built-in account for administering the computer/domain
Guest		Built-in account for guest access to the computer/domain
spirit		
ToshSat		

Groups	Description
Administrators	Members can fully administer the computer/domain
Backup Operators	Members can bypass file security to back up files
Guests	Users granted guest access to the computer/domain
Power Users	Members can share directories and printers
Replicator	Supports file replication in a domain
Users	Ordinary users

7. In **My Computer**, locate and right-click the drive or folder you wish to share and click **Sharing**. Click the **Shared As** radio button and in the **Share Name** field, enter a Share Name (or accept the default). Click the **Permissions** button.



(C:) Properties

○ Not Shared

● Shared As:

Share Name: C_viglen

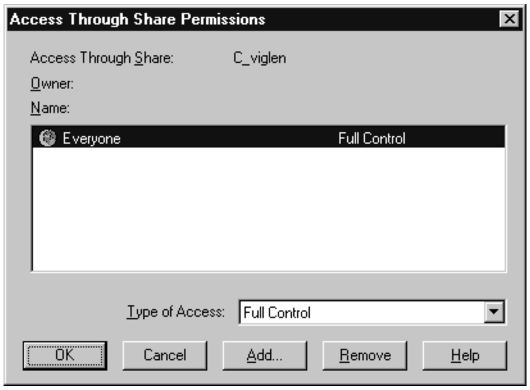
Comment:

User Limit:

● Maximum Allowed

○ Allow Users

8. In the Access Through Share Permissions screen, click the **Add** button. The Add Users and Groups window opens.



Access Through Share Permissions

Access Through Share: C_viglen

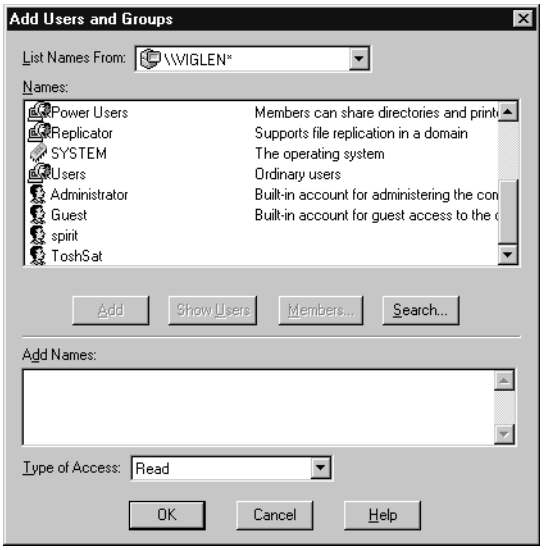
Owner:

Name:

Everyone Full Control

Type of Access: Full Control

9. For each user that you wish to add, find the user's PC on the network (if it is not present, click **Show Users**). Click the user icon and then click the **Add** button.



Add Users and Groups

List Names From: \\VIGLEN*

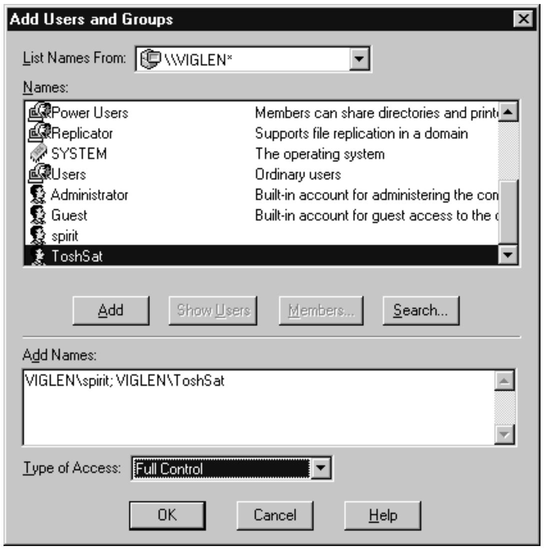
Names:

Power Users	Members can share directories and print
Replicator	Supports file replication in a domain
SYSTEM	The operating system
Users	Ordinary users
Administrator	Built-in account for administering the con
Guest	Built-in account for guest access to the c
spirit	
ToshSat	

Add Names:

Type of Access: Read

10. As you add each user, use the Type of Access pull-down menu to assign the type of access you wish each user to have (for example, Full Control or Read-Only). When all users appear in the Add Names window, click **OK**.



List Names From: \\VIGLEN*

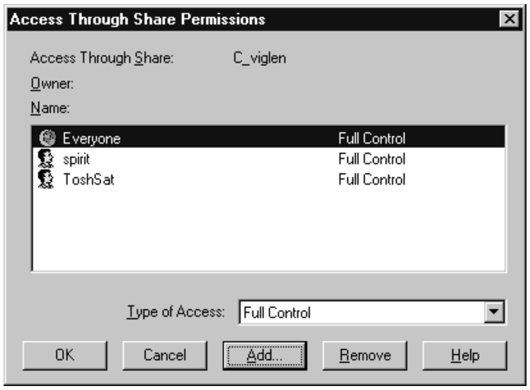
Names:

Power Users	Members can share directories and print
Replicator	Supports file replication in a domain
SYSTEM	The operating system
Users	Ordinary users
Administrator	Built-in account for administering the con
Guest	Built-in account for guest access to the c
spirit	
ToshSat	

Add Names: VIGLEN\spirit; VIGLEN\ToshSat

Type of Access: Full Control

11. Click **OK** to exit Share Permissions.



Access Through Share: C_viglen

Owner:

Name:

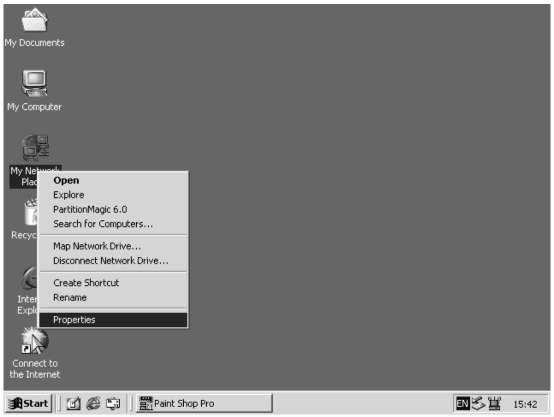
Everyone	Full Control
spirit	Full Control
ToshSat	Full Control

Type of Access: Full Control

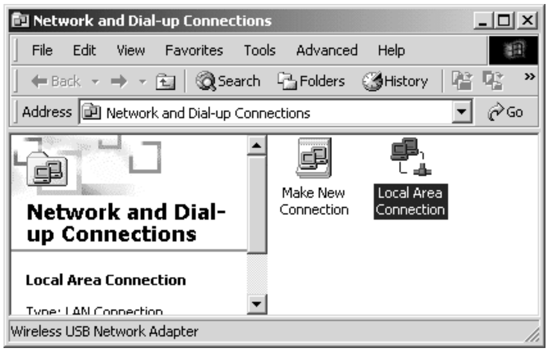
Windows 2000 operating system

Adding PCs to your network

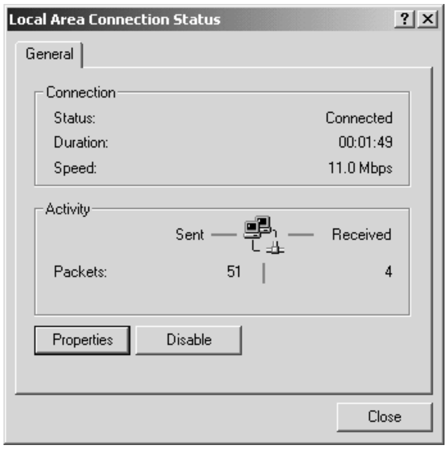
1. Before you add PCs to your network, you must first ensure that networking is enabled. Right-click **My Network Places** and click **Properties**.



2. Networking is enabled if the Local Area Connection icon is present. If it is not present, double-click **Make New Connection** and follow the on-screen instructions.

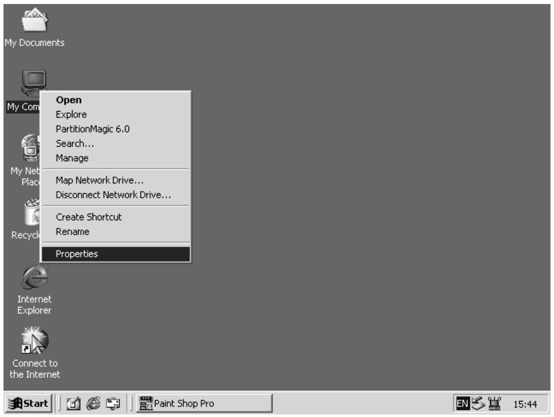


3. When you double-click the Local Area Connection icon, the Local Area Connection Status screen opens.

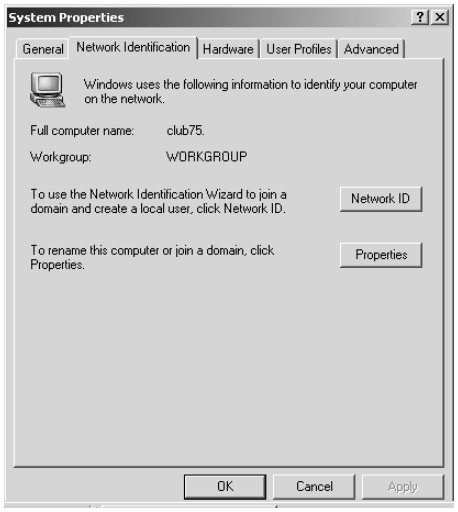


Status: Connected
Duration: 00:01:49
Speed: 11.0 Mbps
Packets: 51 | 4

4. After networking is enabled, you can change your Workgroup name to that of your new network. To do so, right-click **My Computer** and click **Properties**.



5. Select the **Network Identification** tab and click the **Properties** button.



System Properties

General | Network Identification | Hardware | User Profiles | Advanced

Windows uses the following information to identify your computer on the network.

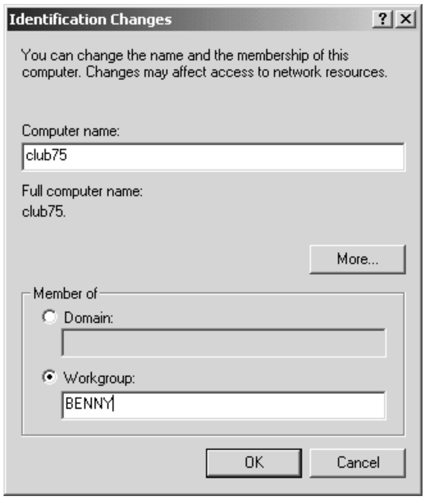
Full computer name: club75.

Workgroup: WORKGROUP

To use the Network Identification Wizard to join a domain and create a local user, click Network ID.

To rename this computer or join a domain, click Properties.

6. In the **Computer name** field, enter a name for the computer. In the **Workgroup** field, enter a name for the workgroup and click **OK**.



Identification Changes

You can change the name and the membership of this computer. Changes may affect access to network resources.

Computer name: club75

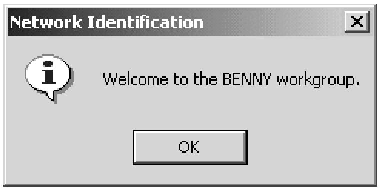
Full computer name: club75.

Member of

○ Domain:

● Workgroup: BENNY

7. The Network Identification welcome screen opens. Click **OK**, then close the Network Identification screen and restart your PC when prompted.



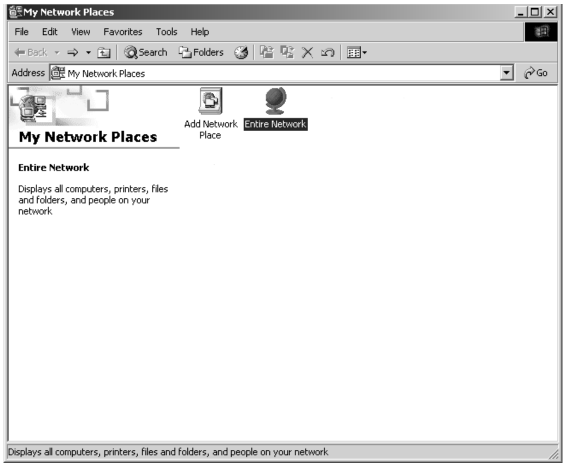
Network Identification

Welcome to the BENNY workgroup.

Accessing PCs on your network

1. To verify that your are connected to the other PCs on your network, double-click the **My Network Places** icon.

2. Double-click **Entire Network**.



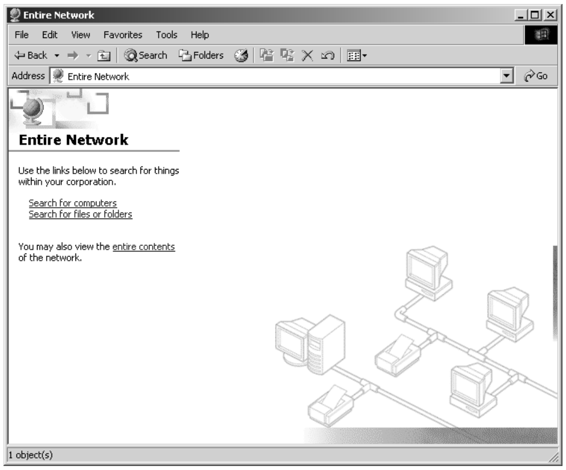
My Network Places

Entire Network

Displays all computers, printers, files and folders, and people on your network

Displays all computers, printers, files and folders, and people on your network

3. Click the **entire contents** link.



Entire Network

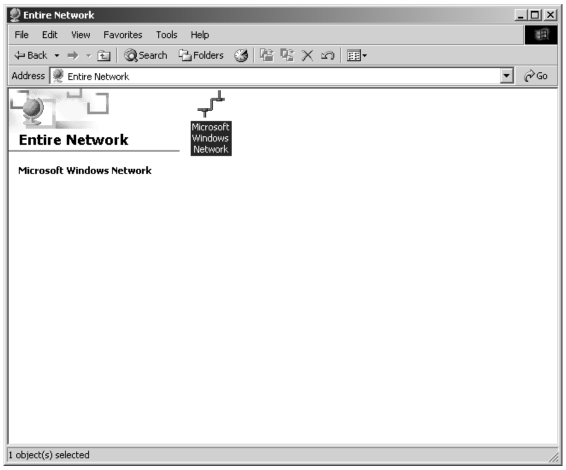
Use the links below to search for things within your corporation.

Search for computers
Search for files or folders

You may also view the entire contents of the network.

1 object(s)

4. Double-click the **Microsoft Windows Network** icon.

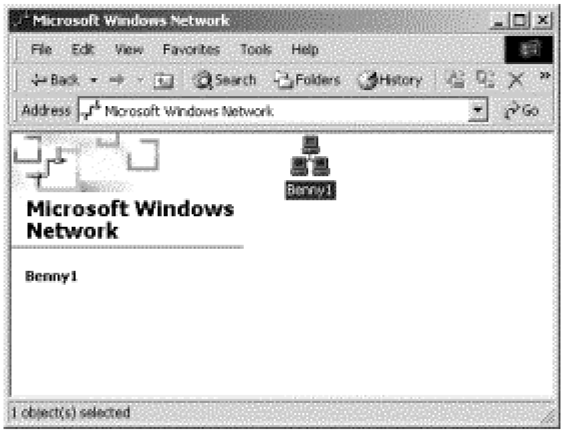


Entire Network

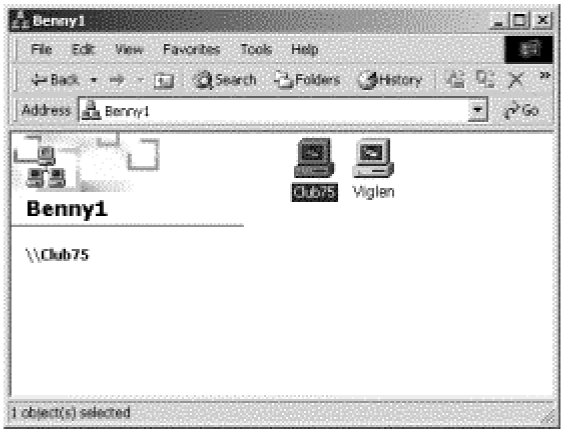
Microsoft Windows Network

1 object(s) selected

5. Double-click the icon with the name of your network.

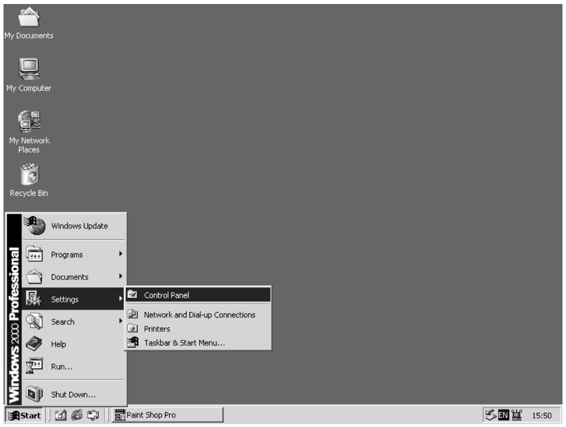

Microsoft Windows Network
File Edit View Favorites Tools Help
Back
Search
Folders
History
Address
Microsoft Windows Network
Go
Benny1
Microsoft Windows Network
Benny1
1 object(s) selected

6. The PCs in your network will be displayed. When file sharing is enabled you will be able to browse the available content of these PCs.

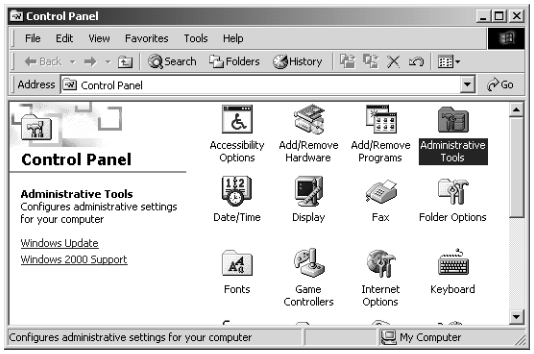


Sharing your files

1. In Windows 2000, before you can share files with other users you must add the other PCs to your User Group. To do so, from the Start menu select **Settings> Control Panels**.



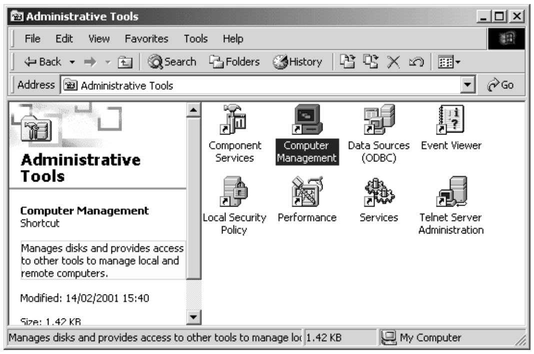
2. Double-click the **Administrative Tools** icon.



Administrative Tools
Configures administrative settings for your computer

Configures administrative settings for your computer

3. Double-click the **Computer Management** icon.



Computer Management
Shortcut

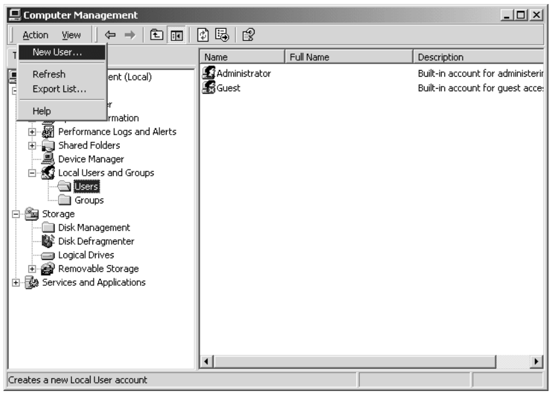
Manages disks and provides access to other tools to manage local and remote computers.

Modified: 14/02/2001 15:40

Size: 1.42 KB

Manages disks and provides access to other tools to manage lo | 1.42 KB

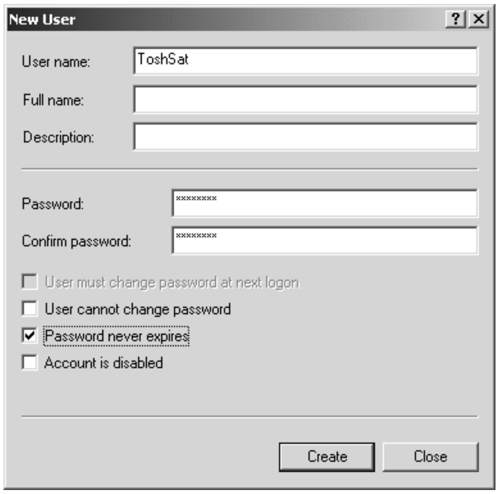
4. Click **Local Users and Groups** and then click on the **Users** folder to highlight it. Click the **Action** button, then click **New User**.



Name	Full Name	Description
Administrator		Built-in account for administerir
Guest		Built-in account for guest acce:

Creates a new Local User account

5. The New User screen opens. In the **User name** field, enter the name of the computer you wish to add. The name must be identical to the name that the PC uses in its network properties. In the Password field, enter a password (recommended). The password should be identical to the one with which the PC logs in to Windows.Click the **Password never expires** checkbox. Click the **Create** button to set up the new user. Repeat these steps for each user you wish to add and when finished, click the **Close** button.



User name: ToshSat

Full name:

Description:

Password: ********

Confirm password: ********

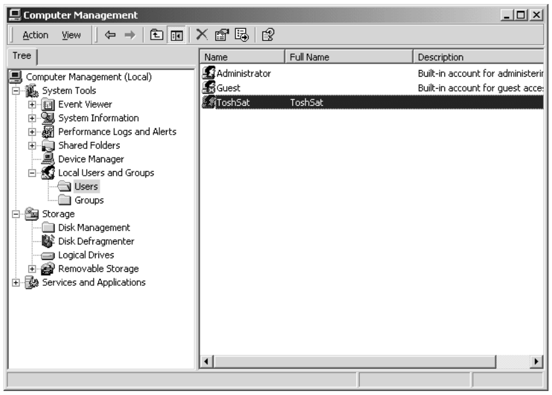
□ User must change password at next logon

□ User cannot change password

☑ Password never expires

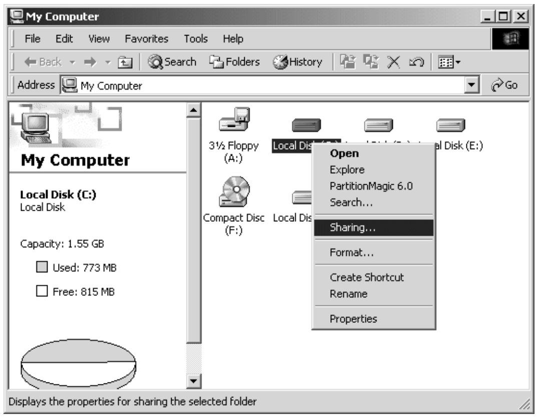
□ Account is disabled

6. The name of each user you have added will now appear in the Users section of the Computer Management screen.



Name	Full Name	Description
Administrator		Built-in account for administerir
Guest		Built-in account for guest acce:
ToshSat	ToshSat	

7. When you have added all users, you can now specify sharing on your chosen drive or folder. To do so, locate your drive or folder, right-click it and click **Sharing**.



My Computer

Local Disk (C:)
Local Disk

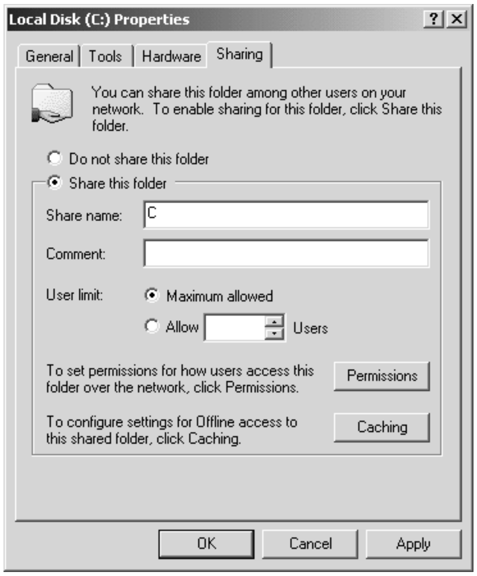
Capacity: 1.55 GB

Used: 773 MB

Free: 815 MB

Displays the properties for sharing the selected folder

8. The Local Disk Properties screen opens. Select the Sharing tab. In the **Share name** field, enter a suitable name for the drive or folder (or accept the default one) and then click the **Permissions** button.



You can share this folder among other users on your network. To enable sharing for this folder, click Share this folder.

○ Do not share this folder

● Share this folder

Share name: C

Comment:

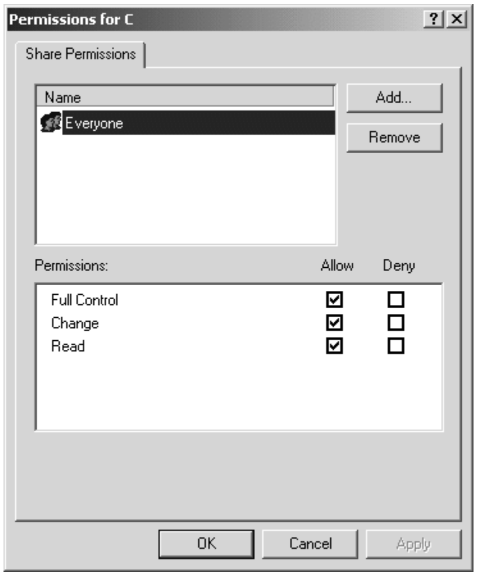
User limit: ● Maximum allowed

○ Allow Users

To set permissions for how users access this folder over the network, click Permissions.

To configure settings for Offline access to this shared folder, click Caching.

9. The Permissions for window opens. Click the **Add** button.



Permissions for C

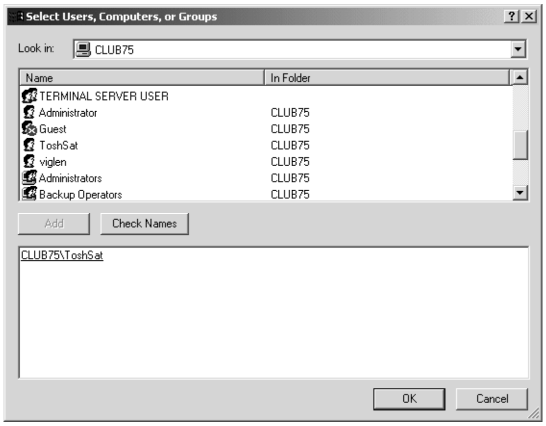
Share Permissions

Name

Everyone

Permissions:	Allow	Deny
Full Control	☑	□
Change	☑	□
Read	☑	□

10. For each PC with which you wish to share a folder, locate the users in the Select Users, Computers, or Groups window and click the icon, then click the **Add** button. Repeat this for each PC with which you wish to share the folder, and then click the **OK** button.



Select Users, Computers, or Groups

Look in: CLUB75

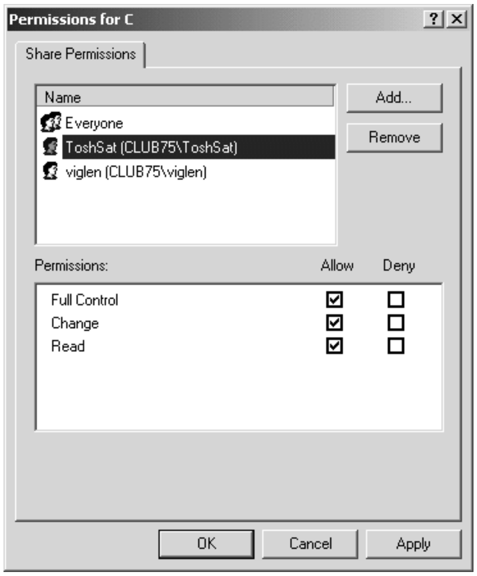
Name	In Folder
TERMINAL SERVER USER	
Administrator	CLUB75
Guest	CLUB75
ToshSat	CLUB75
viglen	CLUB75
Administrators	CLUB75
Backup Operators	CLUB75

CLUB75\ToshSat

11. The users will now appear in the Permissions for window. Click each user icon and assign their access rights in the **Permissions** field (Full Control, Change, or Read). When you have updated access rights for all users, click the **Apply** button and then **OK** to exit.

Your drive/folder will now be shared and display the Shared (hand) symbol.

Local Disk (C:)



Permissions for C

Share Permissions

Name

Everyone

ToshSat (CLUB75\ToshSat)

viglen (CLUB75\viglen)

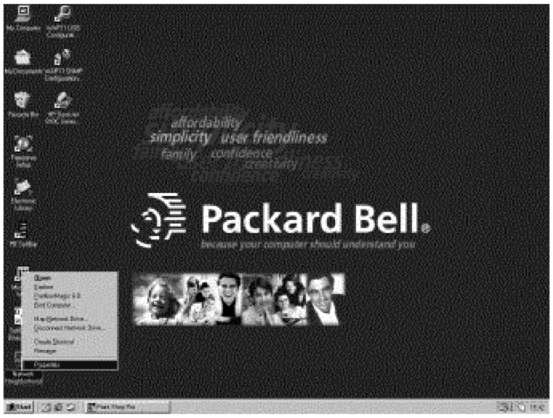
Permissions:	Allow	Deny
Full Control	☑	□
Change	☑	□
Read	☑	□

Printer sharing

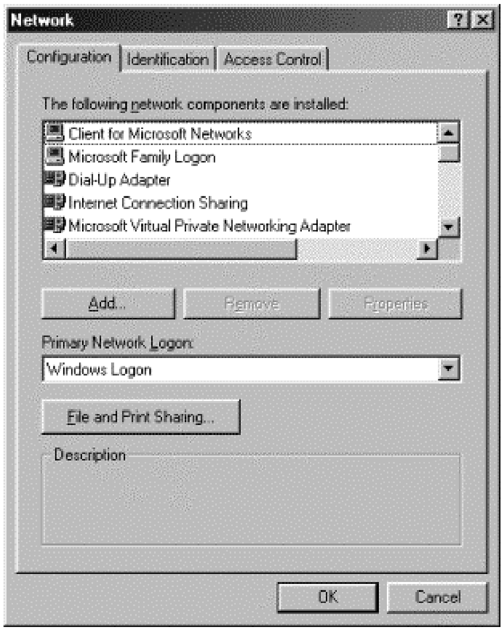
Sharing your printer (Windows 95, 98, and 98 SE)

Print sharing as host

1. Right-click **Network Neighborhood** and click **Properties**.


affordability
simplicity user friendliness
family confidence
creativity
Packard Bell
because your computer should understand you
Properties

2. The Network window opens. In the Configuration tab, click the **File and Print Sharing** button.



Network

Configuration | Identification | Access Control

The following network components are installed:

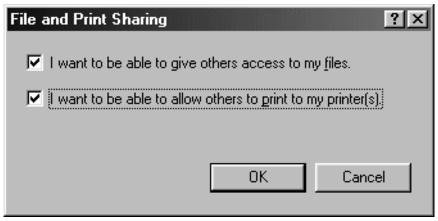
- Client for Microsoft Networks
- Microsoft Family Logon
- Dial-Up Adapter
- Internet Connection Sharing
- Microsoft Virtual Private Networking Adapter

Primary Network Logon:

Windows Logon

3. The File and Print Sharing window opens. Click the **I want to be able to allow others to print to my printer(s)** checkbox and click **OK**.

4. Click **OK** on the Network Properties screen and restart you PC when prompted.

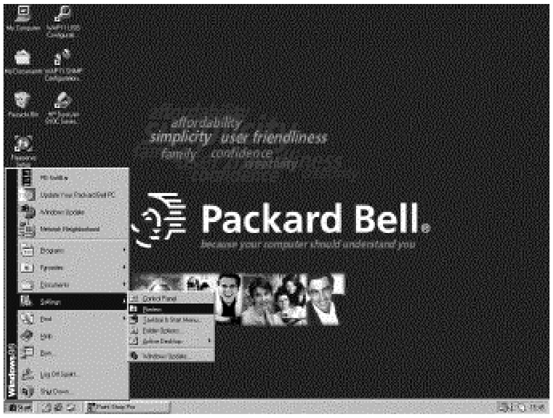


File and Print Sharing

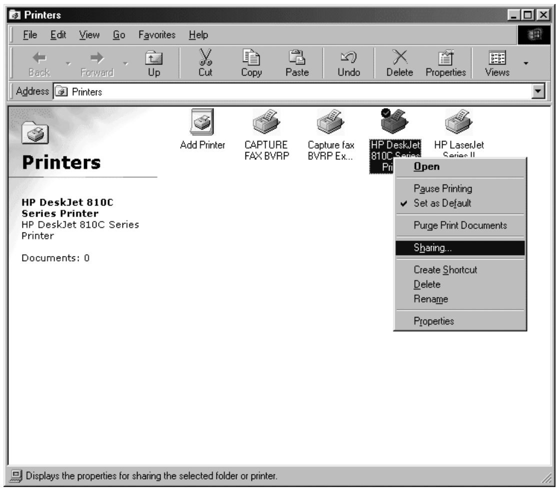
☑ I want to be able to give others access to my files.

☑ I want to be able to allow others to print to my printer(s).

5. When your PC has restarted, from the Start menu select **Settings> Printers**.



6. The Printers window opens. Right-click the printer you wish to share and click **Sharing**.



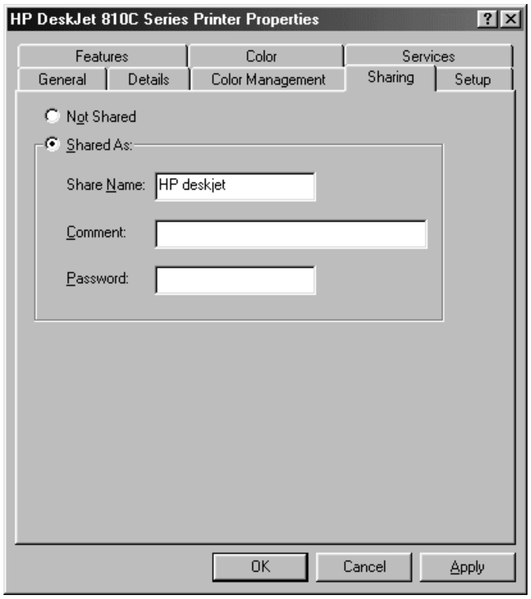
Printers

HP DeskJet 810C Series Printer
HP DeskJet 810C Series Printer

Documents: 0

Displays the properties for sharing the selected folder or printer.

7. In the Sharing tab, click the **Shared As** radio button. In the **Share Name** field, enter a share name for the printer. In the **Password** field, enter an access password (optional). Click the **Apply** button, and then **OK** to exit.



HP DeskJet 810C Series Printer Properties

○ Not Shared

● Shared As:

Share Name: HP deskjet

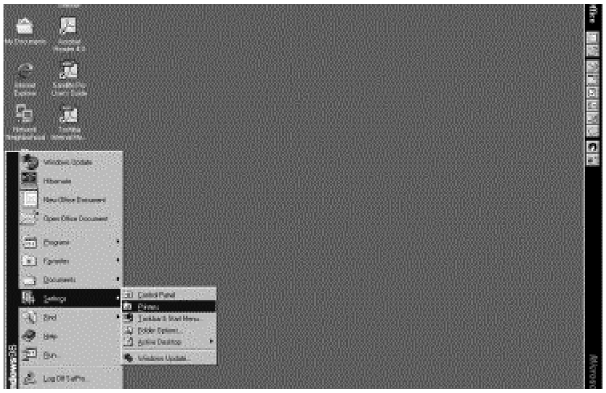
Comment:

Password:

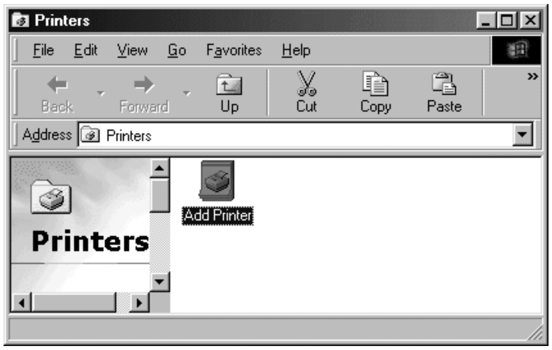
In your Printer folder, the printer will now have the shared (hand) symbol and will be available to everyone on your network.

Print sharing as client

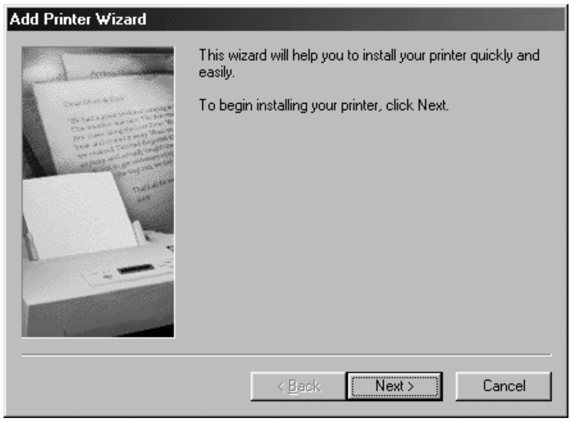
1. When one of your network PCs has a printer configured for sharing, you must add this printer to the printer settings of each PC before they can print to it. From the Start menu, select **Settings> Printers**.



2. The Printers window opens. Double-click the **Add Printer** icon to start the Add Printer Wizard.



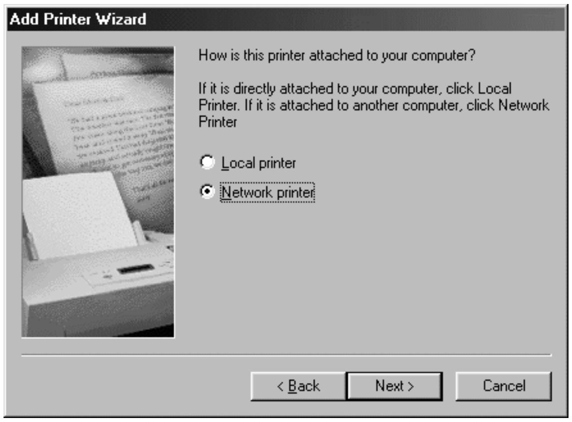
3. Click **Next** to continue.


Add Printer Wizard

This wizard will help you to install your printer quickly and easily.

To begin installing your printer, click Next.

4. Click the **Network printer** radio button and click **Next**.


Add Printer Wizard

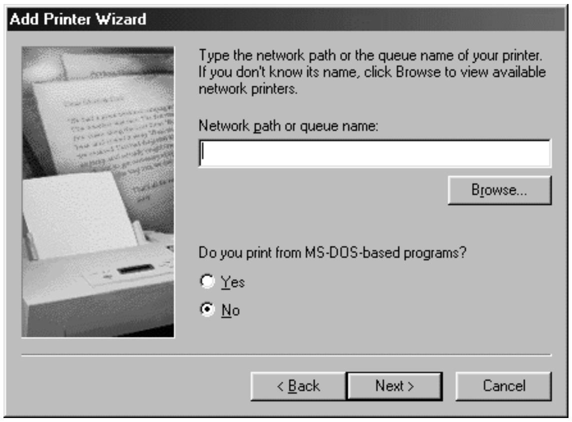
How is this printer attached to your computer?

If it is directly attached to your computer, click Local Printer. If it is attached to another computer, click Network Printer

○ Local printer

● Network printer

5. Click the **Browse** button to locate the networked printer.



Add Printer Wizard

Type the network path or the queue name of your printer. If you don't know its name, click Browse to view available network printers.

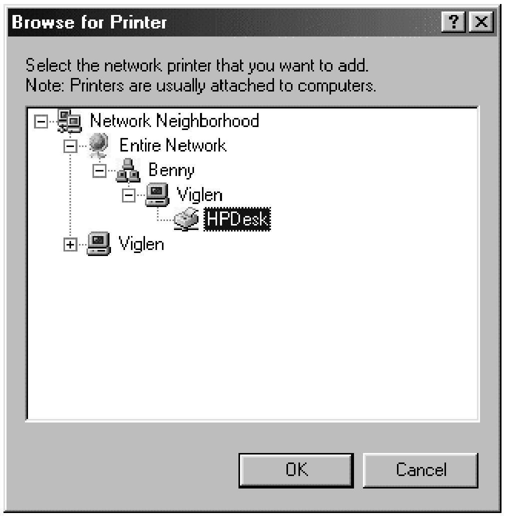
Network path or queue name:

Do you print from MS-DOS-based programs?

○ Yes

● No

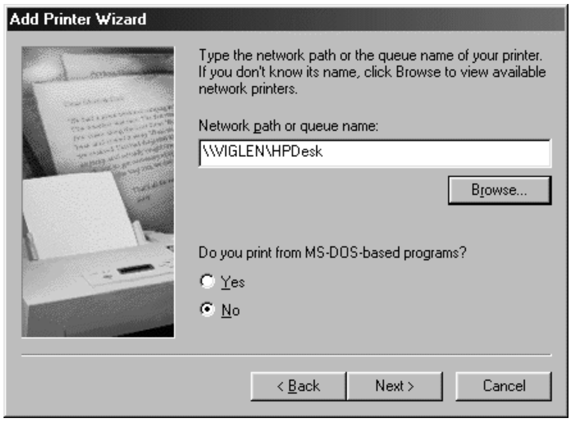
6. Locate the PC to which the printer is attached. Click the printer icon, then click **OK**.



Browse for Printer

Select the network printer that you want to add.
Note: Printers are usually attached to computers.

7. The network path now displays in the **Network path or queue name** field. Click **Next** to continue.



Add Printer Wizard

Type the network path or the queue name of your printer. If you don't know its name, click Browse to view available network printers.

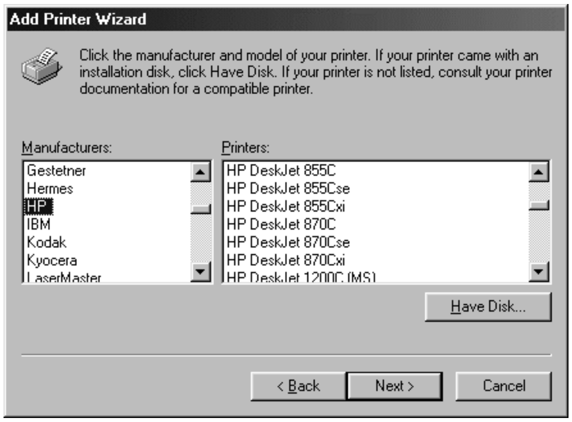
Network path or queue name: \\VIGLEN\HPDesk

Do you print from MS-DOS-based programs?

○ Yes

● No

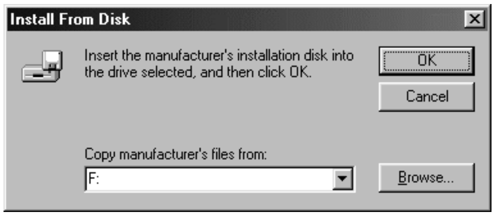
8. The next screen prompts you to select the make and model of your printer. In the **Manufacturers** scroll list, select your printer by make. In the **Printers** scroll list, select your printer by model, then click **Next**. If your printer is not displayed, then click the **Have Disk** button and insert your printer disk.



Add Printer Wizard

Click the manufacturer and model of your printer. If your printer came with an installation disk, click Have Disk. If your printer is not listed, consult your printer documentation for a compatible printer.

9. If you were required to use your printer disk, you will be prompted to enter the location of the printer files (usually the drive letter for whichever drive you are using). Select the path from the **Copy manufacturer's files from** pull-down menu, and click **OK**.

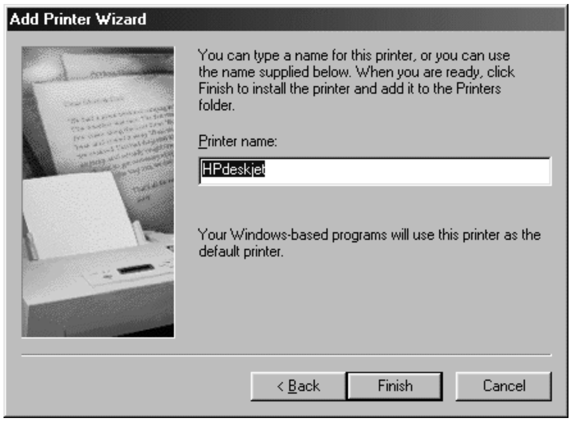


Install From Disk

Insert the manufacturer's installation disk into the drive selected, and then click OK.

Copy manufacturer's files from: F:

10. In the **Printer name** field, enter a name for your printer and click **Finish**.



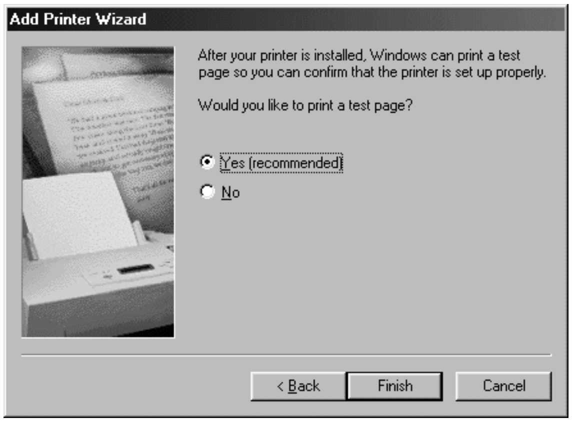
Add Printer Wizard

You can type a name for this printer, or you can use the name supplied below. When you are ready, click Finish to install the printer and add it to the Printers folder.

Printer name: HPdeskjet

Your Windows-based programs will use this printer as the default printer.

11. You will be prompted to print a test page. To print a test page, click the **Yes (recommended)** radio button and click **Finish**.



Add Printer Wizard

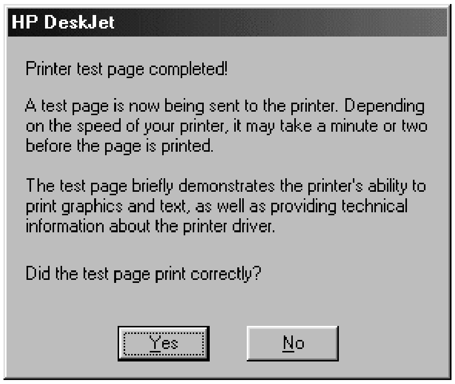
After your printer is installed, Windows can print a test page so you can confirm that the printer is set up properly.

Would you like to print a test page?

● Yes (recommended)

○ No

12. The following confirmation screen opens. Your test page should start printing within less than 60 seconds. If your test page prints successfully, click **Yes**. If it does not print successfully, click **No** to open a troubleshooting tool.



HP DeskJet

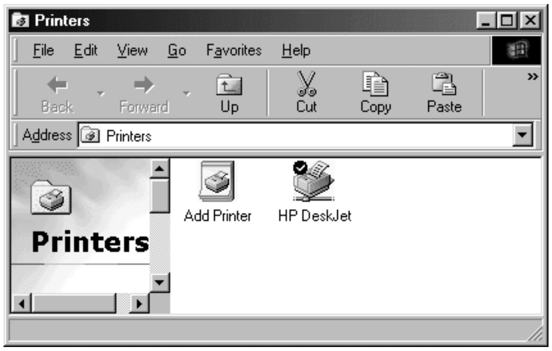
Printer test page completed!

A test page is now being sent to the printer. Depending on the speed of your printer, it may take a minute or two before the page is printed.

The test page briefly demonstrates the printer's ability to print graphics and text, as well as providing technical information about the printer driver.

Did the test page print correctly?

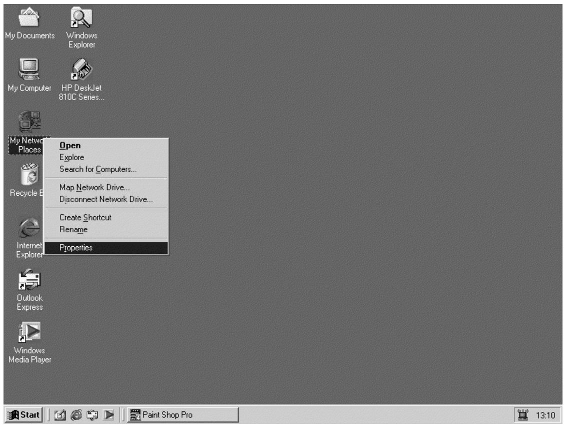
13. If your printer has been set up correctly, it will now appear in your Printers folder.



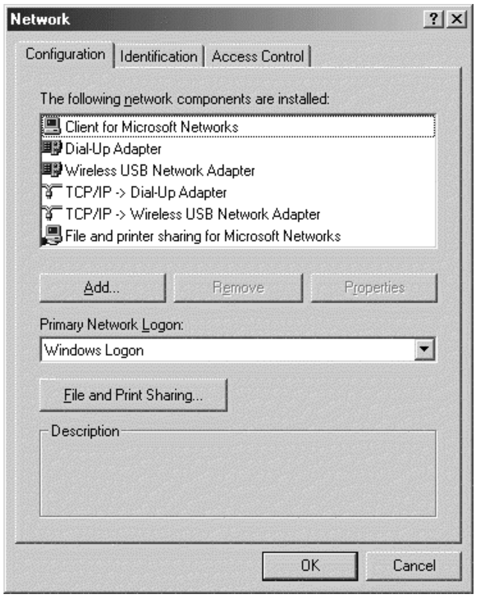
Sharing your printer (Windows ME)

Print sharing as host

1. Right-click the **My Network Places** icon and click **Properties**.



2. The Network window opens. In the Configuration tab, click the **File and Print Sharing** button.



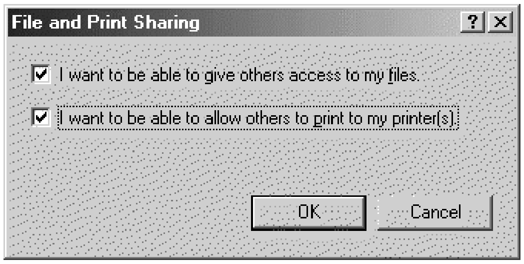
The following network components are installed:

- Client for Microsoft Networks
- Dial-Up Adapter
- Wireless USB Network Adapter
- TCP/IP -> Dial-Up Adapter
- TCP/IP -> Wireless USB Network Adapter
- File and printer sharing for Microsoft Networks

Primary Network Logon: Windows Logon

3. Click the **I want to be able to allow other to print on my printer(s)** checkbox and click **OK**.

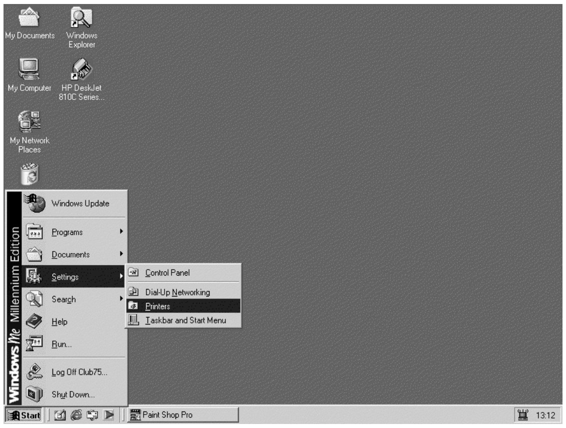
4. In the main Network Properties window, click **OK** and restart your PC when prompted.



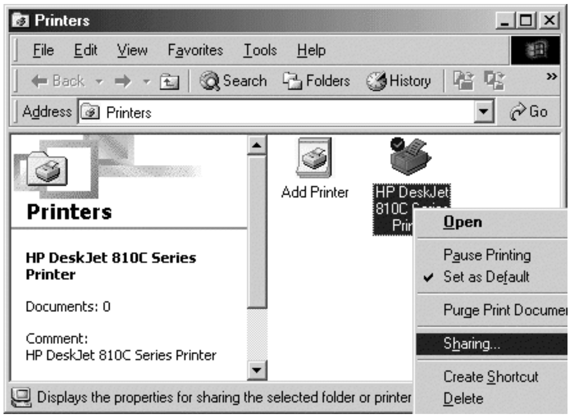
☑ I want to be able to give others access to my files.

☑ I want to be able to allow others to print to my printer(s).

5. When your PC has restarted, from the Start menu select **Settings > Printers**.



6. The Printers window opens. Right-click the printer you wish to share and click **Sharing**.



HP DeskJet 810C Series Printer

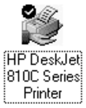
Documents: 0

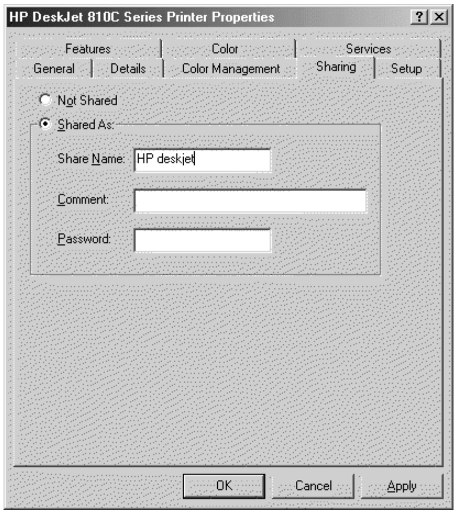
Comment:
HP DeskJet 810C Series Printer

Displays the properties for sharing the selected folder or printer

7. The Printer Properties window opens. In the Sharing tab, click the **Shared As** radio button**.** In the **Share Name** field, enter a suitable name for the printer. In the **Password** field, enter a password (optional) and click the **Apply** button. Click **OK** to exit.

In your Printer folder, the printer will now have the shared (hand) symbol and will be available to everyone on your network.





○ Not Shared

● Shared As:

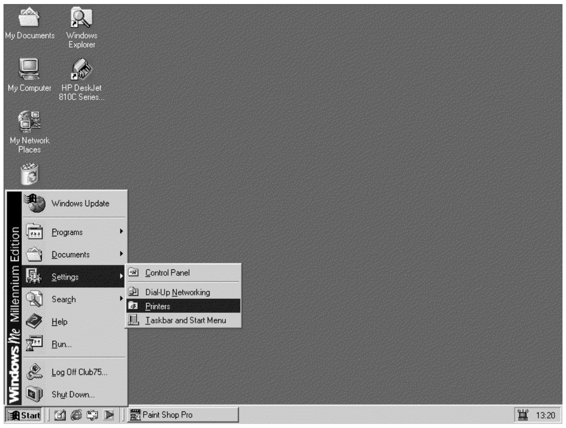
Share Name: HP deskjet

Comment:

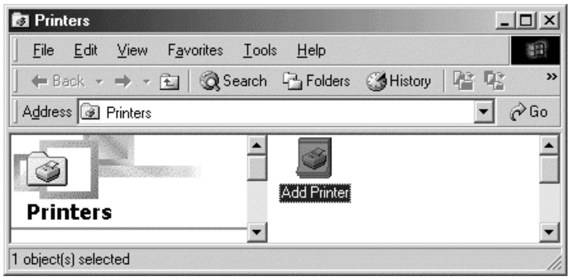
Password:

Print sharing as client

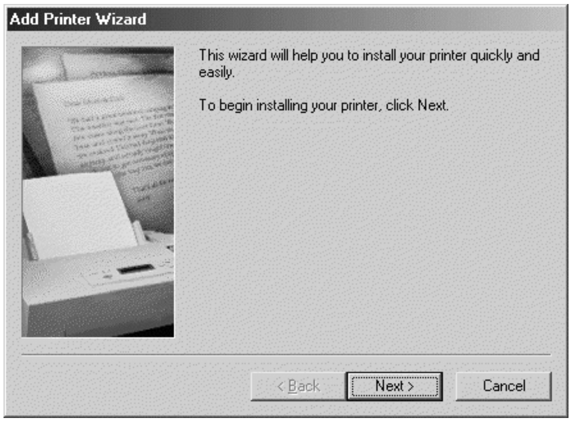
1. From the Start menu, select **Settings> Printers**.



2. The Printers window opens. Double-click the **Add Printer** icon to open the Add Printer Wizard.



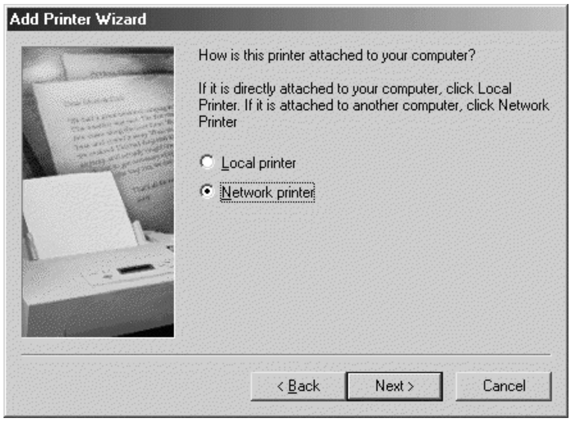
3. Click **Next** to continue.



This wizard will help you to install your printer quickly and easily.

To begin installing your printer, click Next.

4. Click the **Network printer** radio button and click **Next** to continue.



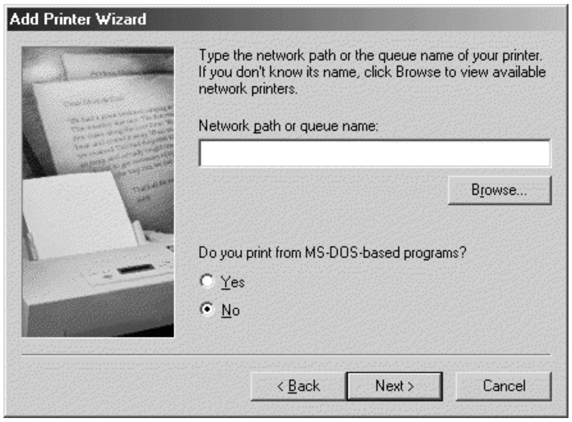
How is this printer attached to your computer?

If it is directly attached to your computer, click Local Printer. If it is attached to another computer, click Network Printer

○ Local printer

● Network printer

5. Click the **Browse** button to locate your network printer.



Type the network path or the queue name of your printer. If you don't know its name, click Browse to view available network printers.

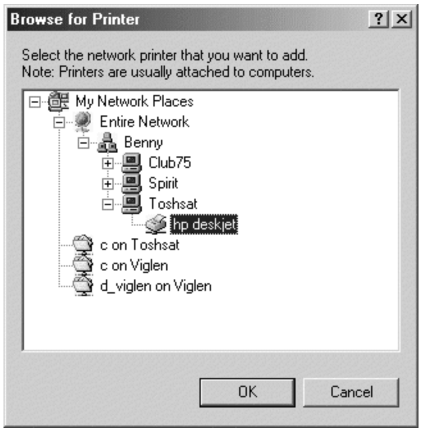
Network path or queue name:

Do you print from MS-DOS-based programs?

○ Yes

● No

6. In the Browse for Printer window, click your printer to select it and click **OK**.

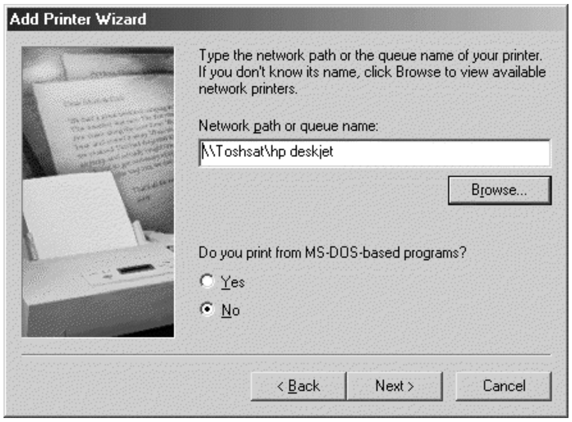


Browse for Printer

Select the network printer that you want to add.
Note: Printers are usually attached to computers.

- My Network Places
  - Entire Network
    - Benny
      - Club75
      - Spirit
      - Toshsat
        - hp deskjet
  - c on Toshsat
  - c on Viglen
  - d_viglen on Viglen

7. The network path for your printer is now displayed in the **Network path or queue name** field. Click **Next** to continue.



Add Printer Wizard

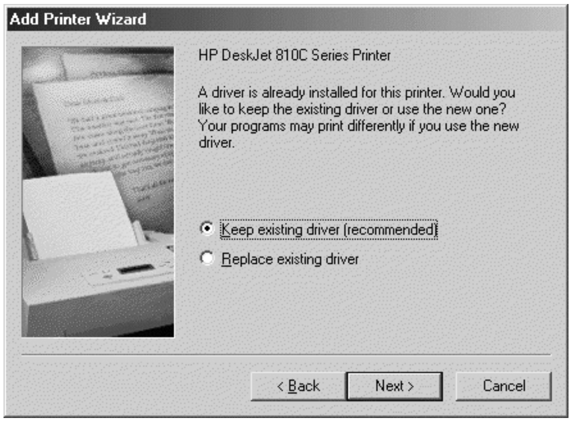
Type the network path or the queue name of your printer. If you don't know its name, click Browse to view available network printers.

Network path or queue name: \\Toshsat\hp deskjet

Do you print from MS-DOS-based programs?

○ Yes
● No

8. If the following screen appears, click the **Keep existing driver (recommended)** radio button. Click **Next** to continue.



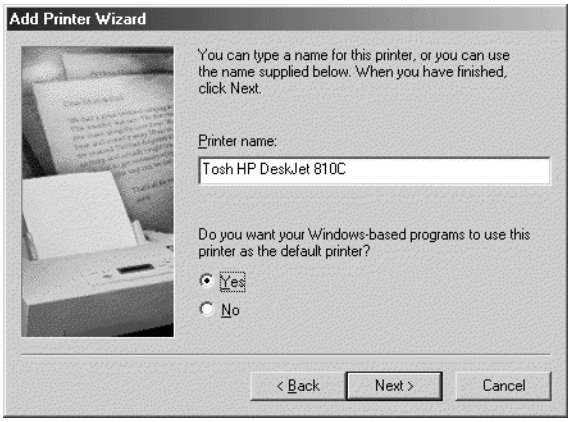
Add Printer Wizard

HP DeskJet 810C Series Printer

A driver is already installed for this printer. Would you like to keep the existing driver or use the new one? Your programs may print differently if you use the new driver.

● Keep existing driver (recommended)
○ Replace existing driver

9. In the **Printer name** field, enter a suitable name for your printer. If you want Windows-based programs to use this printer as the default, click the **Yes** radio button. Click **Next** to continue.



Add Printer Wizard

You can type a name for this printer, or you can use the name supplied below. When you have finished, click Next.

Printer name:

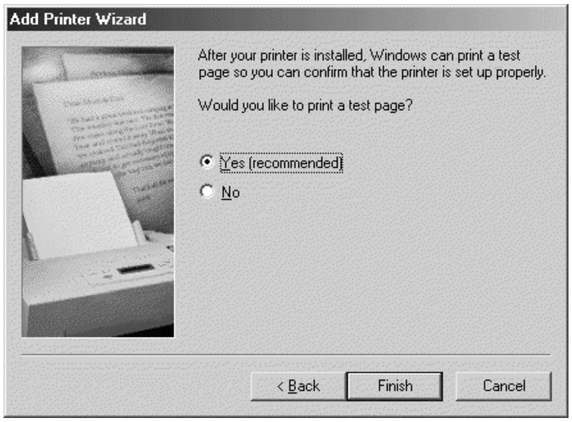
Tosh HP DeskJet 810C

Do you want your Windows-based programs to use this printer as the default printer?

● Yes

○ No

10. You will be prompted to print a test page. To print a test page, click the **Yes (recommended)** radio button and click **Finish**.



Add Printer Wizard

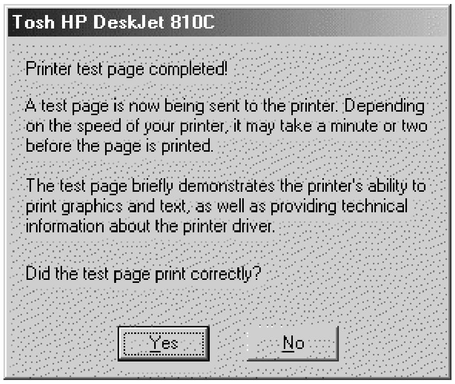
After your printer is installed, Windows can print a test page so you can confirm that the printer is set up properly.

Would you like to print a test page?

● Yes (recommended)

○ No

11. The following confirmation screen opens. Your test page should start printing within less than 60 seconds. If your test page prints successfully, click **Yes**. If it does not print successfully, click **No** to open a troubleshooting tool.



Tosh HP DeskJet 810C

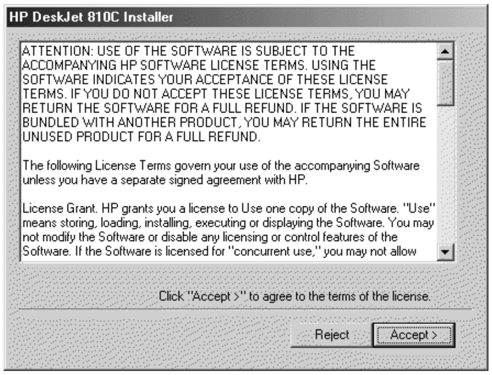
Printer test page completed!

A test page is now being sent to the printer. Depending on the speed of your printer, it may take a minute or two before the page is printed.

The test page briefly demonstrates the printer's ability to print graphics and text, as well as providing technical information about the printer driver.

Did the test page print correctly?

12. If the Terms and Conditions screen opens, click the **Accept** button.



HP DeskJet 810C Installer

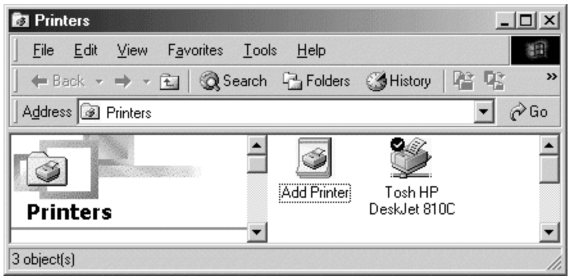
ATTENTION: USE OF THE SOFTWARE IS SUBJECT TO THE ACCOMPANYING HP SOFTWARE LICENSE TERMS. USING THE SOFTWARE INDICATES YOUR ACCEPTANCE OF THESE LICENSE TERMS. IF YOU DO NOT ACCEPT THESE LICENSE TERMS, YOU MAY RETURN THE SOFTWARE FOR A FULL REFUND. IF THE SOFTWARE IS BUNDLED WITH ANOTHER PRODUCT, YOU MAY RETURN THE ENTIRE UNUSED PRODUCT FOR A FULL REFUND.

The following License Terms govern your use of the accompanying Software unless you have a separate signed agreement with HP.

License Grant. HP grants you a license to Use one copy of the Software. "Use" means storing, loading, installing, executing or displaying the Software. You may not modify the Software or disable any licensing or control features of the Software. If the Software is licensed for "concurrent use," you may not allow

Click "Accept >" to agree to the terms of the license.

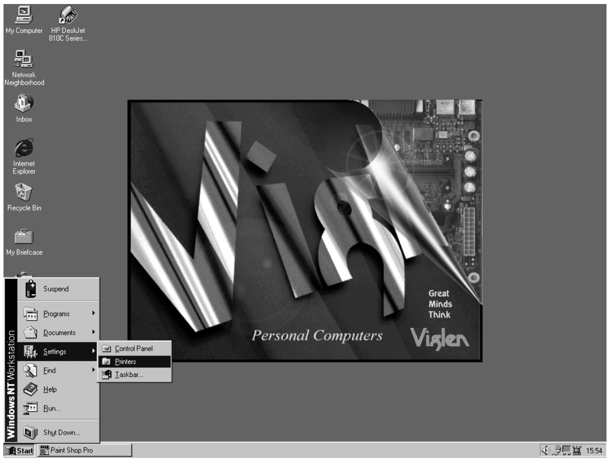
13. The printer will now appear in your Printer folder.



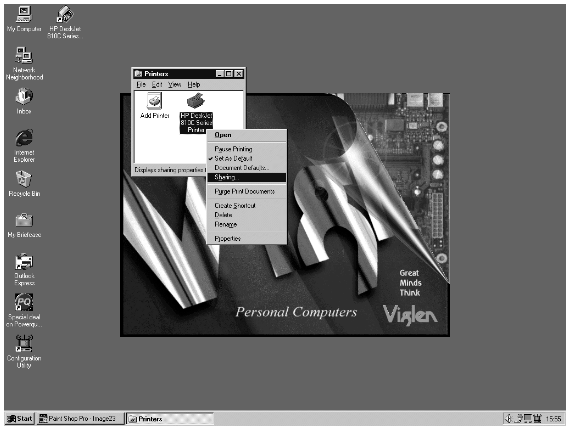
Sharing your printer (Windows NT)

Print sharing as host

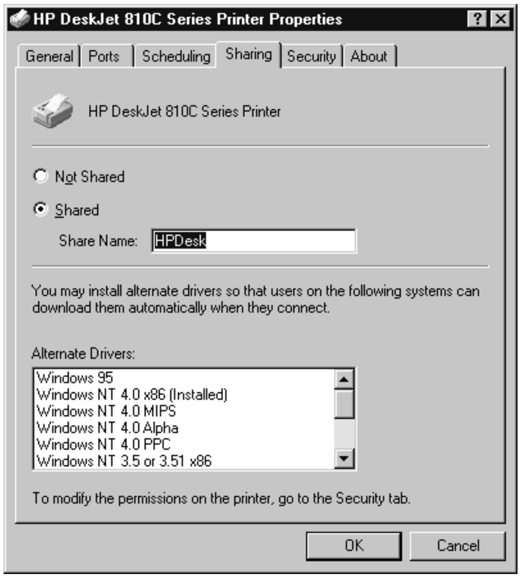
1. From the Start menu, select **Settings> Printers**.



2. In the Printers folder, locate the printer you wish to share, right-click it and click **Sharing**.



3. The Printer Properties window opens. In the Sharing tab, click the **Shared** button. In the **Share Name** field, enter a suitable name for your printer. To install drivers for other users on different operating systems, you can select these in the **Alternate Drivers** scroll list. Click **OK**.



HP DeskJet 810C Series Printer Properties

HP DeskJet 810C Series Printer

○ Not Shared

● Shared

Share Name: HPDesk

You may install alternate drivers so that users on the following systems can download them automatically when they connect.

Alternate Drivers:

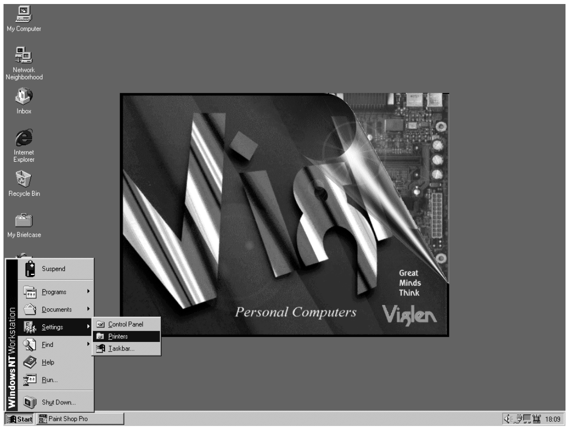
Windows 95
Windows NT 4.0 x86 (Installed)
Windows NT 4.0 MIPS
Windows NT 4.0 Alpha
Windows NT 4.0 PPC
Windows NT 3.5 or 3.51 x86

To modify the permissions on the printer, go to the Security tab.

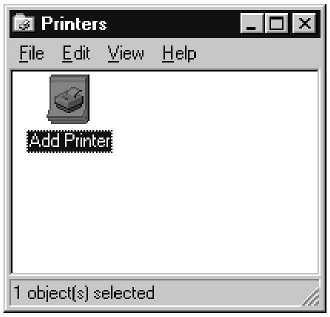
The printer will now have the shared (hand) symbol and will be available to everyone on your network.

Print sharing as client

1. From the Start menu, select **Settings> Printers**.

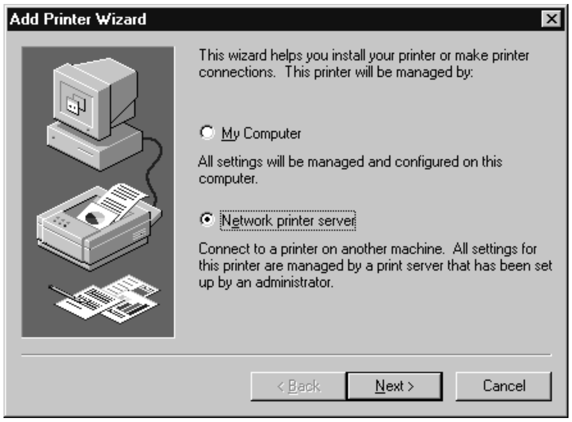


2. In the Printer folder, double-click the **Add Printer** icon to open the Add Printer Wizard.



1 object(s) selected

3. Click the **Network printer server** radio button and click **Next**.



This wizard helps you install your printer or make printer connections. This printer will be managed by:

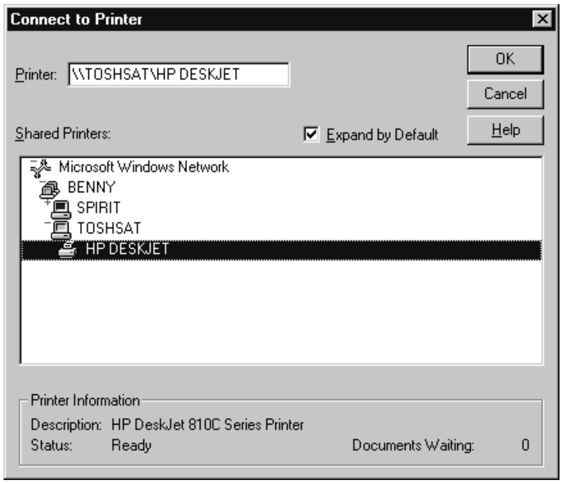
○ My Computer

All settings will be managed and configured on this computer.

● Network printer server

Connect to a printer on another machine. All settings for this printer are managed by a print server that has been set up by an administrator.

4. Browse through your network to find the PC connected to your printer, then click the printer to highlight it and click **OK**.



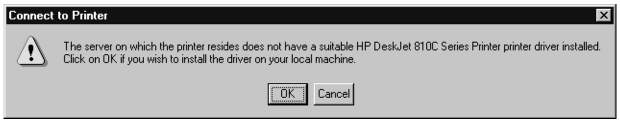
Printer: \\TOSHSAT\HP DESKJET

Shared Printers: ☑ Expand by Default

Microsoft Windows Network
BENNY
SPIRIT
TOSHSAT
HP DESKJET

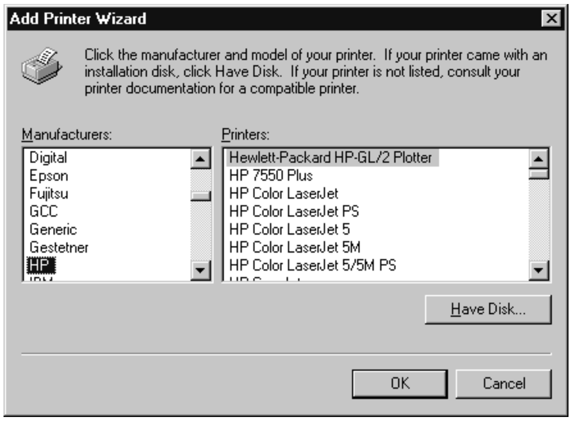
Printer Information
Description: HP DeskJet 810C Series Printer
Status: Ready
Documents Waiting: 0

5. If the drivers for the printer are not already installed, the following message may display. Click **OK**.



The server on which the printer resides does not have a suitable HP DeskJet 810C Series Printer printer driver installed. Click on OK if you wish to install the driver on your local machine.

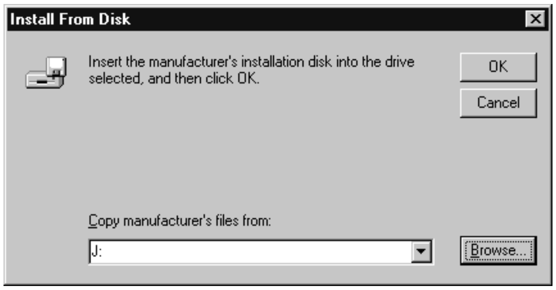
6. The next screen prompts you to select the make and model of your printer. In the **Manufacturers** scroll list, select your printer by make. In the **Printers** scroll list, select your printer by model, then click **Next**. If your printer is not displayed, then click the **Have Disk** button and insert the CD-ROM that came with your printer.



Click the manufacturer and model of your printer. If your printer came with an installation disk, click Have Disk. If your printer is not listed, consult your printer documentation for a compatible printer.

Manufacturers:	Printers:
Digital	Hewlett-Packard HP-GL/2 Plotter
Epson	HP 7550 Plus
Fujitsu	HP Color LaserJet
GCC	HP Color LaserJet PS
Generic	HP Color LaserJet 5
Gestetner	HP Color LaserJet 5M
HP	HP Color LaserJet 5/5M PS

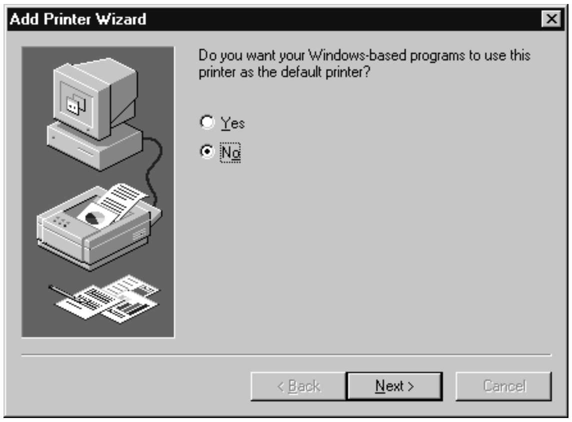
7. Click the **Browse** button to locate your CD-ROM drive and then click **OK**.



Insert the manufacturer's installation disk into the drive selected, and then click OK.

Copy manufacturer's files from: J:

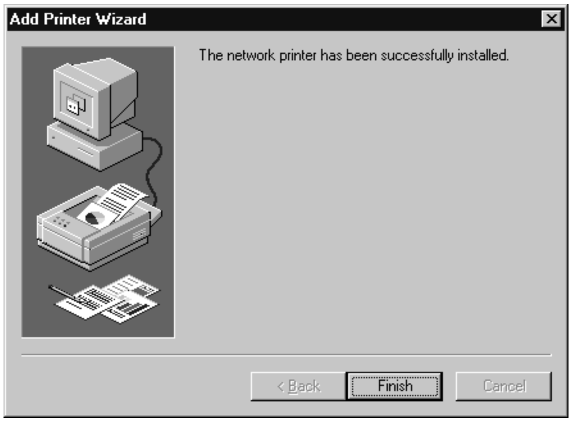
8. If you want Windows-based programs to use this printer as the default, click the **Yes** radio button. Click **Next** to continue.



Do you want your Windows-based programs to use this printer as the default printer?

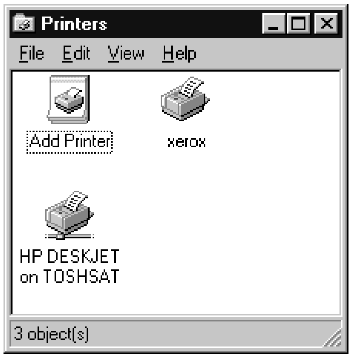
○ Yes
● No

9. The last screen confirms that the printer has been successfully installed. Click **Finish** to exit.



The network printer has been successfully installed.

10. The printer will now appear in your Printer folder.

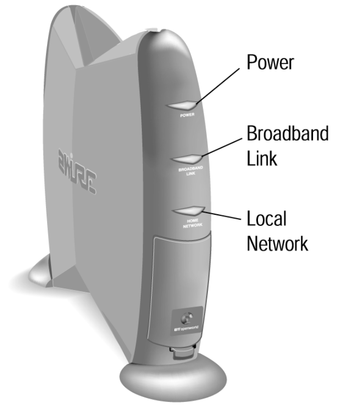


3 object(s)

The Intelligent Gateway Indicator Lights

Intelligent Gateway indicator and status lights

The Intelligent Gateway has three indicator lights that can be used to diagnose installation and connection problems. The following tables describe how to interpret the **POWER**, **BROADBAND LINK**, and **LOCAL NETWORK** lights.



Power light	Operating state
OFF	The Intelligent Gateway is not getting power.
Blinking green	The Intelligent Gateway is powering up.
Solid green	Power is on.
Solid red	System error. Contact Technical Support.

Broadband Link light	Operating state
OFF	No broadband signal is present. The Intelligent Gateway is not plugged into a power outlet, or it is not physically connected to your broadband service.
Blinking orange	The Intelligent Gateway is attempting to establish a physical broadband connection.
Solid red	The Intelligent Gateway has not detected a broadband signal.
Solid orange	The Intelligent Gateway has established a physical broadband connection but was not able to successfully connect to your Internet Service Provider, or has not yet been configured.
Blinking green	The Intelligent Gateway is attempting to establish a connection to your Internet Service Provider.
Solid green	The Intelligent Gateway is fully connected to your Internet Service Provider.

Local Network light	Operating state
OFF	The Intelligent Gateway is not plugged into a power outlet, or it is not connected to any computer via USB, Ethernet, HPNA, or wireless.
ON	The Intelligent Gateway is connected to a computer via USB, Ethernet, HPNA, or wireless.

Diagnosing connection problems

This section describes some connection problems you may encounter with your Intelligent Gateway network and provides suggestions for solving those problems. If the problem you are having is not covered here or in the Help system, or if the suggestions provided do not solve the problem, call the Technical Support number provided with your Intelligent Gateway.

POWER indicator light is not lit

If the **POWER** indicator light is not lit, the Intelligent Gateway is not getting power:

1. Check to see if the power cable is plugged into the power outlet.
2. Make sure the power cord is correctly and securely connected into the Intelligent Gateway.

Note: *If the **POWER** indicator light is red (signifying a system error), or does not light after performing the steps above, contact BT Openworld Customer Care.*

BROADBAND LINK indicator light is red

If the **BROADBAND LINK** indicator light is red, the Intelligent Gateway has not established a connection to your DSL service provider:

1. Verify that a telephone cord is plugged into the **PHONE LINE** port on the Intelligent Gateway and into the *telephone socket with DSL service*.
2. Verify that DSL service is activated by calling your DSL service provider.

LOCAL NETWORK indicator light is not lit

If your networked computers are powered on and the **LOCAL NETWORK** indicator light is not lit, the Intelligent Gateway may not have been connected correctly. Double check the connection diagrams for your particular connection type against your completed Intelligent Gateway setup.

Frequently Asked Questions

This chapter provides frequently asked questions about installation, networking, and Intelligent Gateway configuration and management.

Installation FAQs

What is the best way to connect a second PC to my Intelligent Gateway network?

There are four different ways you can connect a computer to your Intelligent Gateway: Ethernet, HomePNA, direct connect USB, and Wireless. Each connection type has advantages in different circumstances.

When deciding how to connect a second computer to your Intelligent Gateway network there are three things to consider:

- **Does the computer already have a network adapter installed, and if so, what type?** If the computer already has a network adapter installed, it is best to use it rather than go through the time and expense of installing another network interface.
- **How is the first computer connected?** How the first computer is connected may determine how the second computer can be connected or if other equipment is necessary. Use the following table to view the possibilities and restrictions for connecting a second computer. Select the type of connection that the first computer is using in the column on the left, and follow the row across to the right to view the possibilities.

First computer	**Second computer**			
	Ethernet	HomePNA	USB	Wireless
Ethernet	Yes*	Yes	Yes	Yes
HomePNA	Yes	Yes**	Yes	Yes
USB	Yes	Yes	No***	Yes
Wireless	Yes	Yes	Yes	Yes

* Requires the use of an Ethernet hub or switch if the Intelligent Gateway model does not have multiple Ethernet ports.

** Requires the use of a telephone line “Y” adapter so both computers can attach to the LINE port on the back of the Intelligent Gateway.

*** There can be only one direct connection to the USB port on the Intelligent Gateway. If the first computer is connected directly via USB, the second computer cannot be connected via USB.

- **How far is the computer from the Intelligent Gateway?** If the second computer is in the same room, there should be no constraints on a wireless connection. For a direct USB connection, the computer must be within six feet of the Intelligent Gateway. With Ethernet or HomePNA, a cable of appropriate length will be necessary.

If the second computer is not in the same room as your Intelligent Gateway, consider the following:

- Ethernet requires a special cable (Category 5 - Unshielded Twisted Pair). To connect a computer in a different room via Ethernet you must have an Ethernet cable that is long enough, and for safety reasons it should be located out of the way of foot traffic.
- HomePNA requires that a telephone wall socket is located in the same room in which the additional computer will be used, and that the telephone number be the same as the telephone line that is connected to your Intelligent Gateway. Additionally, performance will decrease as the distance to the computer increases, as more devices are connected to the same telephone line, and as the overall amount of cable on the telephone line increases. For optimal performance, it is recommended that you locate computers in your HomePNA network no farther than 300 feet from the Intelligent Gateway.
- Wireless (802.11b) requires that the wireless signal reach to the location where the additional computer is located. The wireless signal will decrease as the distance to the computer increases, and if objects (such as a walls or appliances) obstruct the signal. For optimal performance, it is recommended that you locate computers in your wireless network no farther than 50 feet from the Intelligent Gateway.

How do I connect my second computer using the existing phone lines?

To connect a computer to your Intelligent Gateway network using the existing telephone line, you must have a HomePNA network adapter installed on the computer and access to a telephone wall socket whose telephone number is the same as the telephone line that is connected to the Intelligent Gateway.

Install the HomePNA network adapter in the computer and connect the computer to the telephone wall socket using a telephone wire.

If the computer is in the same room as your Intelligent Gateway, you can connect directly to the Intelligent Gateway’s line using a telephone “Y” connector. If a phone is already connected to the wall socket, you can use a telephone “Y” connector to connect both the phone and the HomePNA adapter to the wall socket.

Note: *If an ADSL Filter is connected between the telephone and the wall socket, make sure the filter is between the telephone and the “Y” connector. If the filter is connected between the HomePNA network adapter and the wall socket, the HomePNA signal will be blocked and a network connection will not be established.*

What is the difference between connecting my computer using Ethernet and direct connect USB?

Your Intelligent Gateway supports four different network connection types: Ethernet (including Ethernet hubs), direct connect USB, HomePNA, and 802.11b Wireless. You can connect to your Intelligent Gateway network using any of these connection types.

To connect using Ethernet, you must have an Ethernet network adapter installed in your computer and an Ethernet cable that is long enough to connect your computer to your Intelligent Gateway.

To connect using USB, you must have a USB cable (a six foot, light gray USB cable is provided with your Intelligent Gateway), the Intelligent Gateway Setup CD, and a computer with an open USB port, running Windows 98, 98SE, ME, 2000, or XP, or Mac 8.6 to 9.x or 10.2 or higher.

Note: *Windows 95, NT, and other versions of Macintosh computers are not supported for direct connect USB.*

How many computers can I connect to my Intelligent Gateway?

The Intelligent Gateway supports up to 250 IP addresses on the Intelligent Gateway network: 32 static and 218 dynamic via DHCP.

Do I need to use a “hub” with my network?

You only need a hub if you wish to connect multiple computers to your Intelligent Gateway network using Ethernet, have used all available Ethernet ports on the Intelligent Gateway to connect additional computers, and your location is not wired with Ethernet (CAT5) cabling. If this is the case, you will need an Ethernet hub/switch.

To connect an Ethernet hub/switch, connect an Ethernet cable from the **LOCAL NETWORK** Ethernet port on the back of your Intelligent Gateway to any port on your Ethernet hub/switch. The Intelligent Gateway auto-senses the connection type so there is no need to worry about using a special cable or connecting it to a special port on the Ethernet hub/switch. Then connect the Ethernet computers to the Ethernet hub/switch with Ethernet cables. However, the Intelligent Gateway allows you to connect computers using any combination of Ethernet, direct USB, HomePNA or Wireless.

Note: *Be careful to connect the computers to the correct ports on the hub/switch with a non-crossover cable if your hub/switch does not support auto crossover. HomePNA, Wireless, and Direct connect USB do not support hubs or switches.*

While running the Setup Wizard, I received the following error message: “Cannot contact configuration server.”

This error message occasionally appears when Internet traffic is particularly heavy. It will not affect the Setup Wizard process.

Networking FAQs

How can I change my network IP range?

You can change the IP address range used by the Intelligent Gateway network by following these steps:

1. From the Intelligent Gateway home page, click the Local Network tab on the top of the Intelligent Gateway user interface.
2. Click the Advanced Settings tab.
3. In the Settings panel, select the IP address scheme you want to use or define your own.
4. Click the **SAVE** button.

Note: *If you change the IP address scheme, you must release and renew the IP addresses on all the devices using DHCP on your Intelligent Gateway network and reconfigure all devices using static IP addressing.*

Can I use static IP addresses for my computers and appliances?

Yes. The Intelligent Gateway reserves the first 32 addresses in the Intelligent Gateway network subnet for static use. By default the Intelligent Gateway uses the non-routable 172.16.0.0 / 255.255.0.0 subnet. Addresses 172.16.1.1 to 172.16.1.32 are reserved for static IP addresses. The Intelligent Gateway’s DHCP server delivers addresses 172.16.1.33 to 172.16.1.250 to dynamic IP clients on your Intelligent Gateway network.

Note: *The Intelligent Gateway Network IP address scheme can also use 192.168.0.0 / 255.255.0.0 and 10.0.0.0 / 255.255.0.0, or you can configure your own subnet.*

Is the Intelligent Gateway compatible with other Internet sharing software?

No. If you have Internet Connection Sharing (ICS) software running on your network, you should disable it before installing your Intelligent Gateway. ICS and Intelligent Gateway will conflict with each if they are both run at the same time.

Does the Intelligent Gateway work with Linux, FreeBSD, and other operating systems?

The Intelligent Gateway will work with network devices that are based on the Internet Protocol (IP), including Linux, FreeBSD, UNIX, and network connected devices.

The Broadband Link light on my Intelligent Gateway is red and I cannot connect to the Internet.

The DSL connection has been interrupted, possibly because of a network outage. The Intelligent Gateway will automatically try to reconnect as soon as it detects a signal is available. If the outage continues, disconnect your Intelligent Gateway from the mains power and then reconnect it.

The Broadband Link light on my Intelligent Gateway is orange and I cannot connect to the Internet.

The PPPoA login has been lost, possibly because of a network outage. The Intelligent Gateway will periodically retry the login to reestablish normal service. If you have changed your PPPoA username or password, you must change the username and password on the Intelligent Gateway. To do so:

1. Click the Broadband Link tab.
2. Click the Advanced Settings tab.

3. In the Broadband Network **Username** field, enter your PPPoA username.
4. In the **Password** field, enter your PPPoA password.
5. In the **Confirm Password** field, re-enter your password.

Computer Configuration FAQs

How do I set my browser's home page to the Intelligent Gateway user interface?

To set your browser's home page to the Intelligent Gateway user interface, find the place in your browser to set the home page address and enter //gateway.2wire.net, or the IP address of your Intelligent Gateway (the default IP address is 172.16.0.1).

Following is detailed information for specific browsers:

PC — Internet Explorer 6.0

1. From the menu bar, select **Tools > Internet Options**.
2. Select the General tab.
3. Enter the address in the Home page box.

PC — Netscape 6.2

1. From the menu bar, select **Edit > Preferences**.
2. Select Navigator in the menu on the left side.
3. Enter the address in the Home page box.

Macintosh — Internet Explorer 5

1. From the menu bar, select **Edit > Preferences**.
2. Select Web Browser / Browser Display from the menu on the left side.
3. Enter the address in the Home page box.

Macintosh — Netscape 4.7

1. From the menu bar, select **Edit > Preferences**.
2. Select Navigator in the menu on the left side.
3. Enter the address in the Home page box.

Where can I obtain drivers for my network adapter?

There are four places to look for network adapter drivers:

- On the CD that came with your network adapter.
- On the CD that was provided with your adapter installation instructions. If your network adapter was provided to you with your Intelligent Gateway, the drivers may be integrated with the Intelligent Gateway installation CD.
- In the Support section of the 2Wire Website: //www.2Wire.com/support, for network adapters provided with your Intelligent Gateway installation kit.
- In the "Download" or "Drivers" section of the Website for the manufacturer of your network adapter.

How do I rename my computers?

You can change the name of your computer by following the instructions listed below for your specific operating system.

Windows — 95, 98, 98SE, ME

1. Right-click the Network Neighborhood icon on your desktop and select Properties.
2. Select the Identification tab.

Windows — NT, 2000, XP

1. Right click the My Computer icon on your desktop and select Properties.
2. Select the Network Identification tab.
3. Click the **Properties** button.

Macintosh — 8.6 to 9.x

1. From the Apple menu, select **Control Panel > File Sharing**.
2. Select the Start / Stop tab.

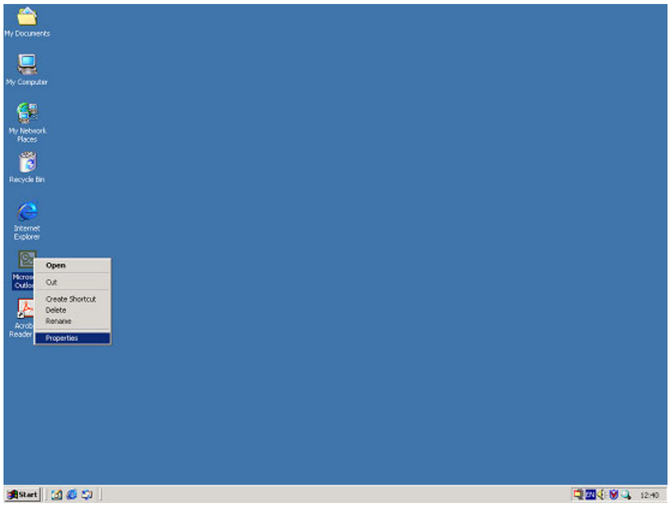
Macintosh — OS X

1. Access System Preferences.
2. Select Sharing.

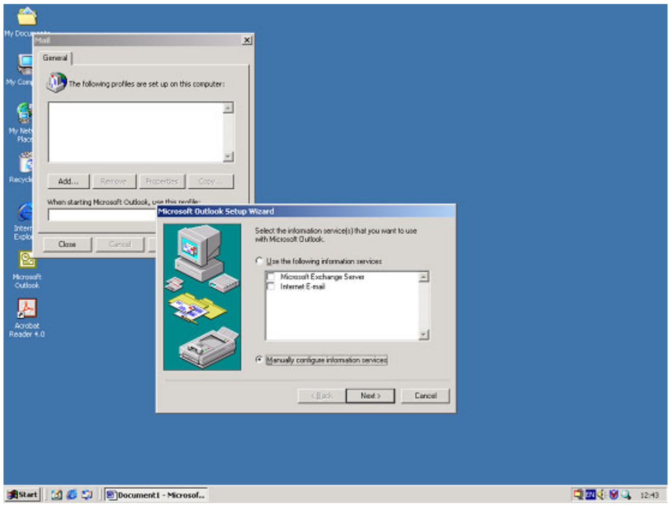
How do I set up an email account using Microsoft Outlook?

The following screens show a first time set up of Microsoft Outlook. If Microsoft Outlook is already set up for use with other mail services (for example, Microsoft Exchange), the appearance of the screens may differ slightly.

1. Right-click the Microsoft Outlook desktop icon and select Properties.



2. Click **Add** and select the **Manually configure information services** radio button. Click **Next**.



The following profiles are set up on this computer:

When starting Microsoft Outlook, use this profile:

Select the information service(s) that you want to use with Microsoft Outlook.

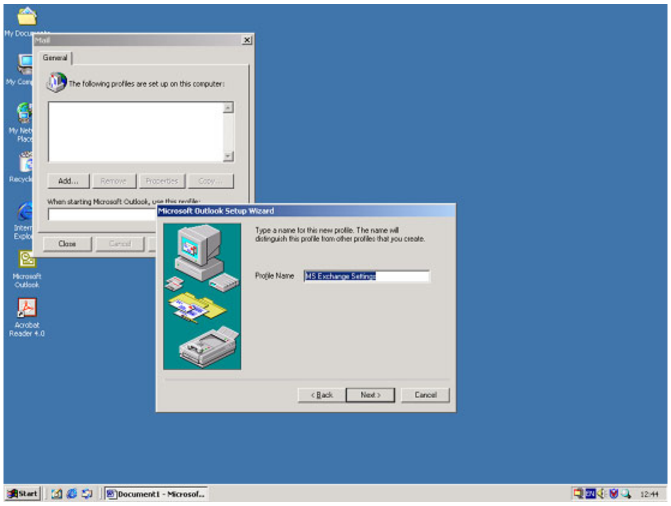
○ Use the following information services:

□ Microsoft Exchange Server

□ Internet E-mail

● Manually configure information services

3. Leave the default **Profile Name** and click **Next**.



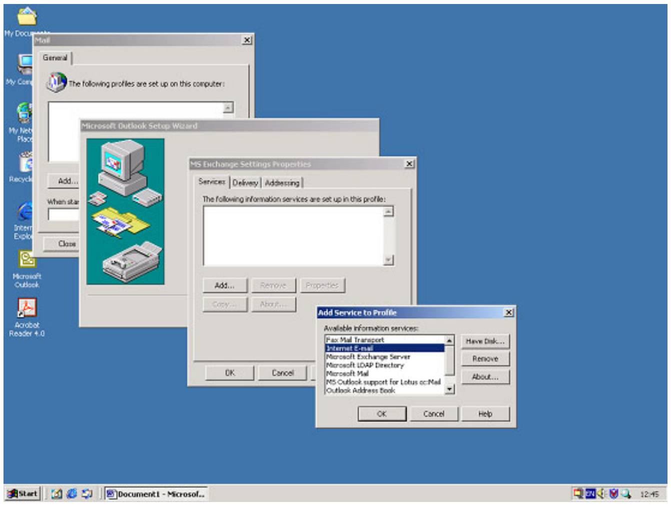
The following profiles are set up on this computer:

When starting Microsoft Outlook, use this profile:

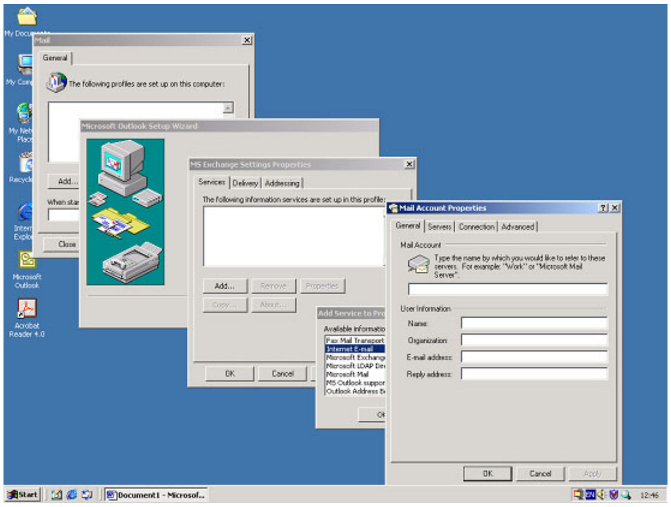
Type a name for this new profile. The name will distinguish this profile from other profiles that you create.

Profile Name: MS Exchange Settings

4. The Add Services to Profile window opens. Select **Internet E-mail** and click **OK**.


Mail
General
The following profiles are set up on this computer:
Microsoft Outlook Setup Wizard
MS Exchange Settings Properties
Services
Delivery
Addressing
The following information services are set up in this profile:
Add...
Remove
Properties
Copy...
About...
OK
Cancel
Add Service to Profile
Available information services:
Fax Mail Transport
Internet E-mail
Microsoft Exchange Server
Microsoft LDAP Directory
Microsoft Mail
MS Outlook support for Lotus cc:Mail
Outlook Address Book
Have Disk...
Remove
About...
OK
Cancel
Help
Start
Document1 - Microsof...
12:45

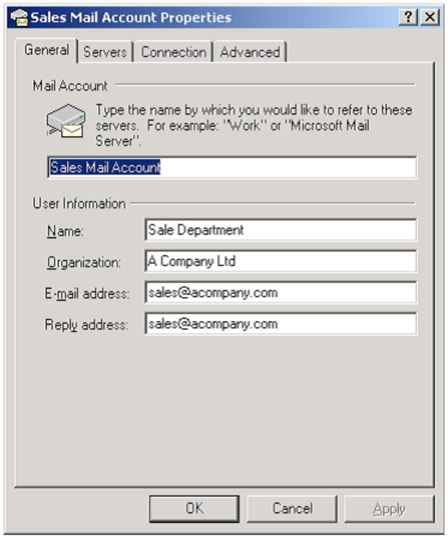
5. The Mail Account Properties window opens.



Note: *If Microsoft Outlook has previously been configured, the preceding steps will be skipped. In this case the first step will be to click the Add button and then select Internet E-mail.*

6. In the Mail Account field, enter the name you want displayed for the email account. In the E-mail address field, enter the email address of the account you are setting up. If you are setting up your BT

Openworld primary mail account, the email address is supplied in your Welcome Pack. You can also enter information in the Name and Organization fields at your discretion (optional).



Mail Account

Type the name by which you would like to refer to these servers. For example: "Work" or "Microsoft Mail Server".

Sales Mail Account

User Information

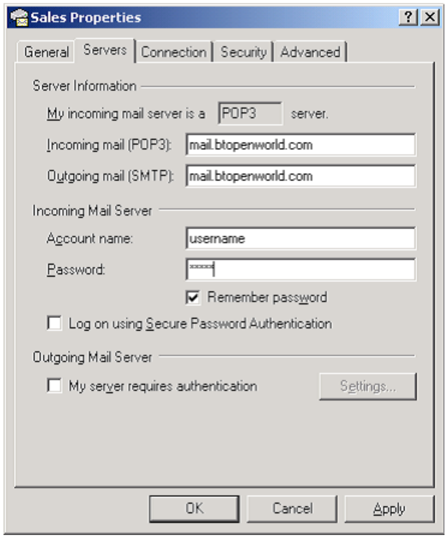
Name: Sale Department

Organization: A Company Ltd

E-mail address: sales@acompany.com

Reply address: sales@acompany.com

7. Click the Servers tab. In the **Incoming mail (POP3)** and **Outgoing mail (SMTP)** fields, enter the incoming and outgoing mail addresses. If you are setting up a BT Openworld mail account, enter mail.btconnect.com.



Server Information

My incoming mail server is a POP3 server.

Incoming mail (POP3): mail.btopenworld.com

Outgoing mail (SMTP): mail.btopenworld.com

Incoming Mail Server

Account name: username

Password: *****

☑ Remember password

☐ Log on using Secure Password Authentication

Outgoing Mail Server

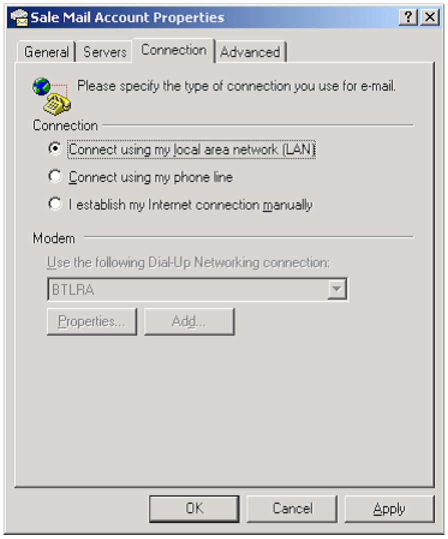
☐ My server requires authentication

Note: *If you are using an alternate mail provider, in the* ***Incoming mail (POP3)*** *field enter the address provided by them. The* ***Outgoing mail (SMTP)*** *address will remain mail.btconnect.com.*

8. In the **Account name** and **Password** fields, enter the account name and password supplied to you by BT Openworld.

Note: *If you are using an alternate mail provider, in the* ***Account name*** *and* ***Password*** *fields enter the information supplied by them.*

9. Click the Connection tab. Click the **Connect using my local area network (LAN)** radio button. Click **OK**.



Sale Mail Account Properties

Please specify the type of connection you use for e-mail.

Connection

● Connect using my local area network (LAN)

○ Connect using my phone line

○ I establish my Internet connection manually

Modem

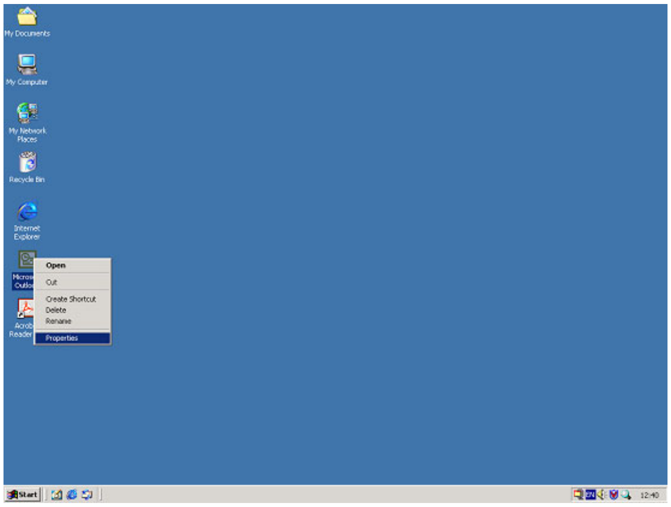
Use the following Dial-Up Networking connection:

BTLRA

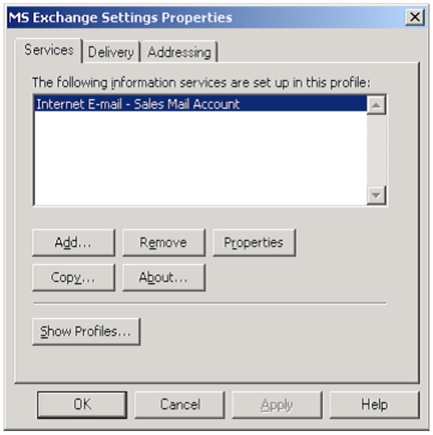
Depending on the current set-up of Microsoft Outlook, you may need to add a personal folder so Microsoft Outlook knows where to store mail. If Microsoft Outlook has previously been configured, this may not be necessary.

To add a personal folder, follow these steps.

1. Right-click the Microsoft Outlook desktop icon. Select Properties.



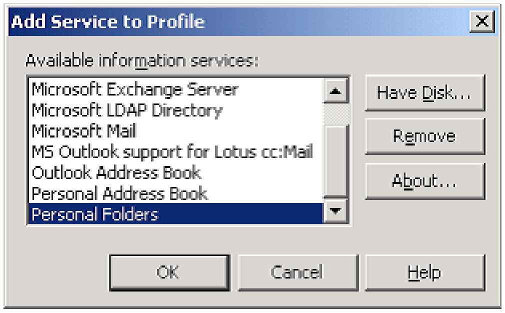
2. In the MS Exchange Settings Properties window, click **Add**.


MS Exchange Settings Properties

The following information services are set up in this profile:

Internet E-mail - Sales Mail Account

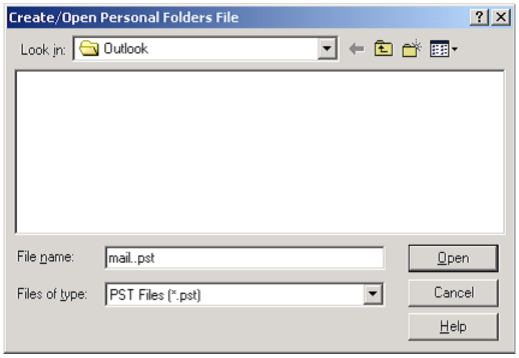
3. In the Add Service to Profile window, select Personal Folders and click **OK**.


Add Service to Profile

Available information services:

Microsoft Exchange Server
Microsoft LDAP Directory
Microsoft Mail
MS Outlook support for Lotus cc:Mail
Outlook Address Book
Personal Address Book
Personal Folders

4. In the **File name** field, enter a name for the folder.



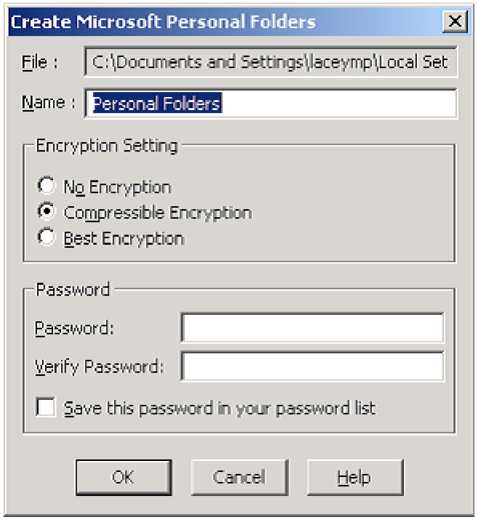
Create/Open Personal Folders File

Look in: Outlook

File name: mail.pst

Files of type: PST Files (*.pst)

5. Click **OK**.



Create Microsoft Personal Folders

File : C:\Documents and Settings\laceymp\Local Set

Name : Personal Folders

Encryption Setting

○ No Encryption
● Compressible Encryption
○ Best Encryption

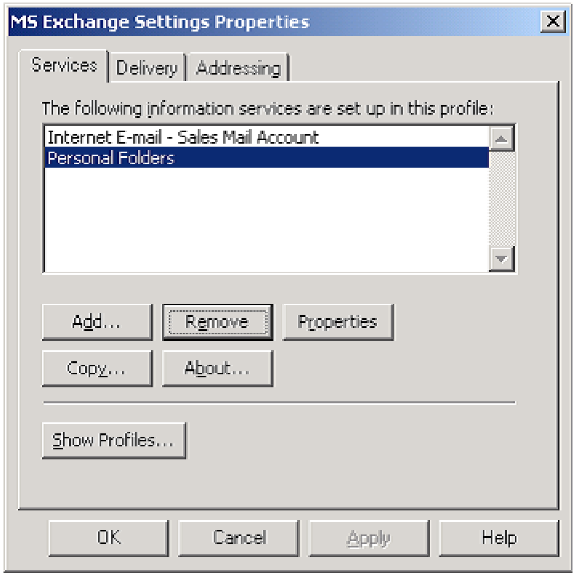
Password

Password:

Verify Password:

□ Save this password in your password list

6. Click **OK** to conclude set-up.

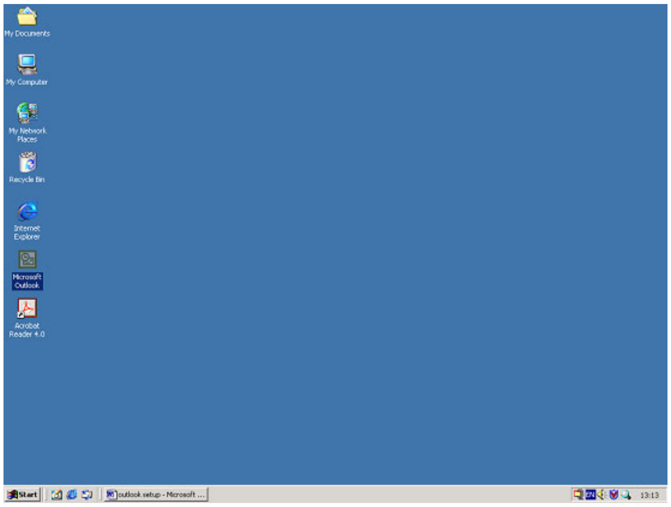


MS Exchange Settings Properties

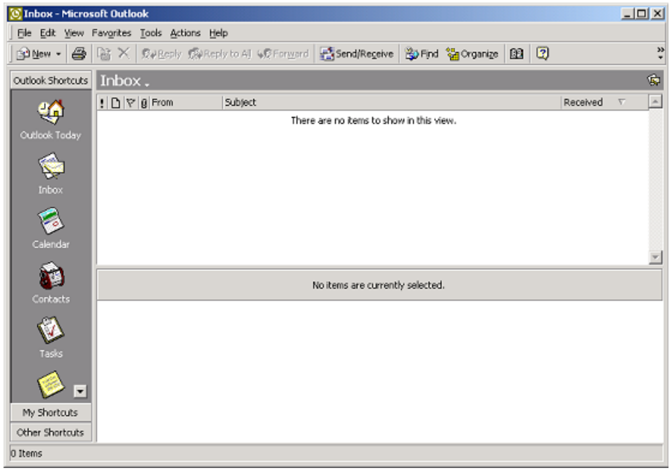
The following information services are set up in this profile:

Internet E-mail - Sales Mail Account
Personal Folders

To verify your set-up, double-click on the Microsoft Outlook desktop icon to run Microsoft Outlook.



Verify that the Inbox is displayed. Click **Send/Receive** to collect email. Check for any error messages.



There are no items to show in this view.

No items are currently selected.

How do I set my browser to accept cookies?

Warning: Changing your cookie settings may have privacy and security implications. Make sure you understand these implications before changing your cookie settings.

Following is detailed information for specific browsers:

PC — Internet Explorer 6.0

1. From the menu bar, select **Tools > Internet Options**.
2. Select the Privacy tab.
3. Click the **Advanced** button.

PC — Netscape 6.2

1. From the menu bar, select **Edit > Preferences**.
2. Select Privacy & Security in the menu on the left side.

Macintosh — Internet Explorer 5

1. From the menu bar, select **Edit > Preferences**.
2. Select Receiving Files / Cookies in the menu on the left side.

Macintosh — Netscape 4.7

1. From the menu bar, select **Edit > Preferences**.
2. Select Advanced from the menu on the left side.

How do I configure my wireless card for a static IP address?

The Intelligent Gateway supports both Dynamic and Static IP addressing on your Intelligent Gateway network. The Intelligent Gateway is a DHCP server and will automatically assign an IP address to a network device upon request. However, you can manually configure a static IP address for any device on your Intelligent Gateway network.

The first 32 addresses (.1 to .32) in the address range are allocated to static IP addresses. The next 218 addresses (.33 to .250) are allocated to the Intelligent Gateway's DHCP server to deliver to dynamic clients. The last 4 addresses are reserved (.251 to .254).

Following are the settings for the three network IP range options offered by the Intelligent Gateway:

	Default Settings	**Option 1**	**Option 2**
Static	172.16.1.1 - .32	192.168.1.1 - .32	10.0.1.1 - .32
Dynamic	172.16.1.33 - .250	192.168.1.33 - .250	10.0.1.33 - .250
Reserved	172.16.1.251-.254	192.168.1.251-.254	10.0.1.251-.254
Subnet	255.255.0.0	255.255.0.0	255.255.0.0
Default Gateway	172.16.0.1	192.168.0.1	10.0.0.1
DNS	172.16.0.1	192.168.0.1	10.0.0.1

How do I know whether my PC has a network adapter that can work with the Intelligent Gateway?

In a Microsoft Windows computer you can check to see if you have a network adapter installed in your computer by accessing the Control Panel and clicking the Network Control application. If an Ethernet, HomePNA, or 802.11b wireless adapter is listed, it can be used to connect to your Intelligent Gateway network. On a Macintosh computer, access the Control Panel and select TCP/IP. Use the Connect via: pull-down menu to see if an Ethernet, HomePNA, or 802.11b wireless (AirPort) network adapter is installed.

During USB install on Windows 2000 a warning message pops up. Is this important?

You may see a pop-up warning message during the installation of the driver for the direct connect USB connection to your Intelligent Gateway. The warning appears because the driver has not yet received its Windows certification. The driver has been fully tested and is compatible with Windows 98, 98 SE, ME, and Windows 2000 operating systems.

I have more than one type of network interface card in my computer, and I'm having network connection problems. What should I do?

Although computer operating systems support two or more concurrent network adapters (dual/multiple home), it can cause confusion as to which network adapter the computer communicates with. To minimize network connection problems, disable all network adapters except the one connected to the Intelligent Gateway network.

Configuration and Management FAQs

How do I remove the inactive computers from the Intelligent Gateway user interface?

The Intelligent Gateway user interface will display them as inactive for two days after computers or network devices have been removed from your Intelligent Gateway network. After two days they will automatically be removed from the user interface.

You can manually remove them by performing the following steps:

1. From the Intelligent Gateway user interface, click the Local Network tab.
2. Click the Advanced Settings tab.
3. In the Settings panel, deselect the **Show inactive devices in network list** checkbox.

Note: *When the **Show inactive devices in network list** checkbox is deselected, the Intelligent Gateway will not display the inactive devices on the pages where network lists are displayed. However, inactive devices will continue to appear in the drop down selection list for Firewall pass-through settings if an application is mapped for that computer. This allows you to unmap the application when the computer is no longer on your Intelligent Gateway network.*

Note: *If you have Internet Access Control and Content Screening settings configured for a computer, the settings will be retained even though the computer is no longer displayed on the network lists of the Intelligent Gateway user interface. When a computer is reconnected to the Intelligent Gateway network, they will regain their defined settings.*

How do I access the Intelligent Gateway management page?

The Management and Diagnostic Console (MDC) is used for advanced troubleshooting. It can be accessed by entering //homeportal/management in the browser address bar.

What is the maximum number of ports that I can open for a game?

You can have up to 64 entries in the firewall pass-through table. If you have one port per entry, you can have up to 64 ports opened. However, each entry can open a range of ports for allowing up to over 65,000 ports to be open.

Why are my FTP downloads slow?

Connections across the Internet are subject to various network connection speeds. When you make a connection to a Website or an FTP server there is no guarantee of the overall connection speed. If you are experiencing a slow download from an FTP server you can disconnect and reconnect in an attempt to get a higher connection speed. However, if the FTP server's connection to the Internet is slow, this will always be the limitation.

Windows XP FAQs

Windows XP includes a PPPoA client. Should I use it?

No. The Intelligent Gateway has a built-in PPPoA client. The Intelligent Gateway PPPoA client software is completely independent from Windows XP and eliminates the need for the Windows XP PPPoA client. When a Windows XP computer is part of an Intelligent Gateway network, the Windows XP PPPoA client should be disabled. This is the default setting.

Does the firewall included with Windows XP conflict with the Intelligent Gateway?

The Windows XP software firewall (Internet Connection Firewall or ICF) can be enabled on each network card connected to your computer. Enabling ICF has no effect on the Intelligent Gateway installation process. However, if ICF is active on the network interface connected to the Intelligent Gateway, it will prevent the Windows XP computer from appearing in the list of networked devices on the Intelligent Gateway home page. This is a result of the Windows XP firewall blocking local polling packets sent to it from the Intelligent Gateway. These packets are used to determine if a computer is active on the network.

My Windows XP computer does not appear on the Intelligent Gateway home page. What happened?

The most likely cause is that the Windows XP firewall (ICF) is enabled. The Windows XP firewall is blocking local polling packets sent to it from the Intelligent Gateway. These packets are used to determine if a computer is active on the network. For an ICF-enabled computer to appear in the network list, you must configure ICF to respond to network polling.

Since Windows XP has a firewall, do I need the Intelligent Gateway firewall?

As with all software firewalls, Windows XP Internet Connection Firewall (ICF) is a complement to the Intelligent Gateway's embedded firewall but is not a substitute. Since the Intelligent Gateway is custom software running on a compact, real-time operating system, it is far less susceptible to attack than large, general consumer operating systems such as Windows. It is a hardware firewall that provides a level of protection that cannot be afforded by a firewall running on a networked computer. Because the Intelligent Gateway is optimized for networking and firewall functions, it can perform with greater efficiency than Windows and without slowing the performance of your computer. Because of its central position in the network, the Intelligent Gateway firewall protects all of your computers including those with other operating systems (such as Windows 98 or ME). In addition, instead of having to go to each computer to manage the firewall settings, management and configuration of the Intelligent Gateway firewall is easily performed. Information about all network activity can be viewed in one location.

When I upgrade to Windows XP, do I have to change the name of my computer? Will changing the name affect my Intelligent Gateway network?

When upgrading to Windows XP, you will have to change the name of your computer only if your computer name contains spaces. Spaces in the computer name are no longer valid under Windows XP. After the upgrade is complete, the computer will appear on the Intelligent Gateway home page with the new name. Otherwise, this change will not affect your Intelligent Gateway network.

Windows XP is supposed to provide new networking functionality. Do I still need my Intelligent Gateway?

Window XP supports Windows Internet Connection Sharing (ICS). Using ICS requires that you dedicate one computer to act as the “connection sharing” computer for your network. This computer must be left on and connected to the Internet at all times for other computers in the network to have access. Running ICS consumes valuable resources on the connection sharing computer and any interruption in its operating system or networking software will cause all computers on the network to lose Internet access. Using ICS requires the use of several different network adapters on the central computer, one for the Internet connection and one for each of the desired network technologies (HomePNA, wireless, Ethernet, etc.). The Intelligent Gateway is a specialized firewall gateway that is designed to efficiently and securely manage a network.

What is the Windows XP Home Networking Wizard and should I run it?

The Windows XP Home Networking Wizard is a tool that can be used to configure your computer for networking. Using this wizard is not necessary and is not recommended for Intelligent Gateway networks. To configure your computer and Intelligent Gateway network, follow the instructions included with your Intelligent Gateway or provided to you by your service provider.

I ran the Home Networking Wizard and now my network is not working.

Use of the Windows XP Home Networking Wizard in and of itself will not cause the connection to the Intelligent Gateway to be lost. The most likely problem is that the Home Networking Wizard has enabled Internet Connection Sharing (ICS) on your Windows XP computer. ICS is incompatible with an Intelligent Gateway network and must be disabled for your network to work properly. Consult the Windows XP help system for instructions on how to disable Internet Connection Sharing (ICS) on your computer.

To configure your computer to work with the Intelligent Gateway network, follow the instructions included with your Intelligent Gateway or provided to you by your service provider.

Will I be able to use Windows XP Professional Remote Desktop (Remote Assistance) if the XP computer to be controlled is behind an Intelligent Gateway?

Yes. Windows XP Professional allows you to connect to another computer. Once connected, you can send chat messages, view screens, and remotely control the other computer.

If a computer is connecting from the Internet to a Window XP computer on the Intelligent Gateway network, you must configure your Intelligent Gateway to allow access through the Intelligent Gateway firewall. To do so, set up your Intelligent Gateway to allow XP Remote Desktop hosting for your Windows XP computer. Starting from the Intelligent Gateway home page, click the Local Network tab, and then Firewall Settings. Select the computer with Windows XP and add "XP Remote Desktop" to the hosted applications list. For more information, refer to your Intelligent Gateway documentation.

No special configuration is needed to allow a computer on the Intelligent Gateway network to remotely control another computer on the Internet. The Intelligent Gateway's firewall automatically allows traffic from the Intelligent Gateway network to the Internet.

Can I use Windows Messenger on a computer that is behind the Intelligent Gateway?

At this time, only the instant messaging function of Windows Messenger is supported for those computers that are part of an Intelligent Gateway network. Advanced functions such as audio, video, whiteboard, and file transfer are not supported except for computers in DMZplus mode. For more information about how to enable DMZplus for a computer, refer to your Intelligent Gateway documentation.

Why can't I upgrade my Intelligent Gateway software from a computer running Windows XP or Internet Explorer 6?

Due to a browser policy change in the latest version of Microsoft Internet Explorer, you may receive a message indicating that the Intelligent Gateway upgrade process cannot be completed. The Intelligent Gateway upgrade process requires the use of "session" or temporary cookies. To reach the upgrade page, you must enable the use of session cookies in your browser. See the Internet Explorer help files for more information on cookies and for instructions on how to change your browser security settings to allow the use of session cookies.

Glossary

A

Access Point. A device that transports data between a wireless network and a wired network. With the help of the system, a wireless base station is an example of an access point that acts between a wireless node and with other wired PCs and peripherals.

ADSL. See Asymmetric Digital Subscriber Line.

American National Standards Institute (ANSI). A non-governmental organization delegated with the responsibility of developing and publishing standards for transmission codes, protocols, and high-level languages for use in the United States.

American Standard Code for Information Interchange (ASCII). A coding method that assigns specific letters, numbers, punctuation, and control codes to a combination of 0s and 1s in a byte. ASCII is the code by which most all personal computers encodes and translates data. ASCII was developed by the American National Standards Institute (see above).

Analog. A continuously varying signal or wave. Telephone transmission and/or switching that is not digital.

ANSI. See American National Standards Institute.

Applet. Small computer programs that can be downloaded quickly and used by computers with a Java-capable browser.

ASCII. See American Standard Code for Information Interchange.

Asymmetric Digital Subscriber Line (ADSL). A group of DSL technologies that are asymmetric, thereby reserving more downstream bandwidth (coming to the user from the Internet) than upstream bandwidth (going from the user to the Internet). This type of DSL is advantageous for residential users that do not need the same bandwidth speed in both directions. Also see DSL

Asynchronous Transfer Mode (ATM). A method of data transportation whereby fixed-length cells are sent over a switched network. Because of its uniform handling of services, one network can meet the needs of many broadband users, for the receipt of voice, video, and data.

ATM. See Asynchronous Transfer Mode.

B

Backbone. The part of a communications network that handles the major traffic using the highest-speed – and often longest – paths in the network.

Bandwidth. A measure of the width or capacity of a communications channel. Greater bandwidth allows communication of more information in a given period of time. Bandwidth is generally described either in terms of analog signals in units of Hertz (Hz), which describes the maximum number of cycles per second, or in terms of digital signals in units of bits per second (bps).

Bit. The basic unit in data communications, represented as either a one or a zero. When discussing digital data, a small "b" refers to bits, and a capital "B" refers to bytes.

Bit Rate. The number of bits of data transmitted over a phone line per second.

Broadband. Broadband is the largest size bandwidth category, meaning that there are the most channels of data moving over a single communication medium, thus information such as data, voice, and video can be received and sent most quickly.

Byte. A compilation of bits. ASCII code uses seven information bits and one parity bit for error control, while EBCDIC standards call for eight information bits. Other less common standards call for more or less bits in a byte.

C

CAP. See Carrierless Amplitude Phase.

Carrier. A signal of a specific frequency which is modulated to transmit information.

Carrierless Amplitude Phase (CAP). A type of quadrature amplitude modulation, used for some types of DSL, that stores pieces of a modulated message signal in memory and then reassembles the parts in the modulated wave.

Category 5. Also known as CAT5. A category of cabling that is used for local area networks with voice and data needs.

Central Processing Unit (CPU). The core of a computer, which uses a stored program to manipulate information.

Circuit-switched Network. A type of network in which a continuous link is established and reserved between a source and a receiver. This type of network is used in telephony applications to ensure minimal delay and to reserve an appropriate level of transmission capacity for the call. Most phone conversation takes place on a circuit-switched network.

Compression. The process of reducing the representation of information. This is often needed in order to transmit a specific audio, video, or data file without using a large amount of transmission time or capacity.

CPE. See Customer Premises Equipment.

CPU. See Central Processing Unit.

Customer Premises Equipment (CPE). Any piece of equipment in a communication system that resides on the customer's premises. Examples include modems, television set-top boxes, telephones and televisions.

D

Data Link. The communications link used for data transmission from a source to a destination. For example, your telephone is a data link.

Data Transfer Rate. The average number of bits per unit of time passing in a data transaction.

Dedicated Connection. A communication link that operates constantly.

DHCP. See Dynamic Host Configuration Protocol.

Dial-up Connection. A data communication link that is established when the communication equipment (e.g. a modem) dials a phone number and negotiates a connection with the equipment on the other end of the link.

Digital Signal. A signal that takes on only two values, off or on, typically represented by "0" or "1." Digital signals require less power but (typically) require more bandwidth than analog.

Digital Subscriber Line Access Multiplexer (DSLAM). A device found in telephone company telephone exchanges that takes a number of DSL subscriber lines and concentrates them onto a single ATM line.

Discrete Multi-Tone Modulation (DMT). A method of transmitting data on copper phone wires that divides the available frequency range into 256 sub-channels or tones, and which is used for some types of DSL.

DMT. See Discrete Multi-Tone Modulation.

DNS. See Domain Name System.

Domain Name System (DNS). The protocol used for assigning text addresses (such as www.bt.com) for specific computers and computer accounts on the Internet.

DSLAM. See Digital Subscriber Line Access Multiplexer.

Dynamic Host Configuration Protocol (DHCP). A TCP/IP protocol that allows servers to assign IP addresses dynamically to PCs and workstations. The PC or workstation "borrows" the IP address for a period of time, then the IP address returns to the DHCP server for reassignment.

E

E-1. A dedicated digital communication link provided by a European telephone company that offers 2.048 Megabits per second of bandwidth, commonly used for carrying traffic to and from private business networks and Internet service providers.

Echo Cancellation. The elimination of reflected signals ("echoes") in a two-way transmission created by some types of telephone equipment, used in data transmission to improve the bandwidth of the line.

Encapsulation. The technique used to layer protocols.

Ethernet. A type of local area network that operates over twisted wire and cable at speeds of up to 10 Mbps.

F

Fiber Optics. Thin strands of ultrapure glass that can be used to carry light waves from one location to another.

Filter. A device which transmits a specific frequency and stops all other frequencies.

Firewall. A security product that employs a combination of hardware and software to prevent unauthorized users or traffic from the Internet from gaining access onto a private local area network (LAN).

Frame Relay. A high-speed packet switching standard used in wide area networks (WANs), often to connect local area networks (LANs) to each other, with a maximum bandwidth of 44.725 Megabits per second.

Frequency. The rate at which an electromagnetic waveform (or electrical current) alternates, usually measured in Hertz (Hz).

G

Gigabyte. 1,000,000,000 bytes, or 1,000 Megabytes. See Byte.

Graphical User Interface (GUI). A computer operating system that is based upon icons and visual relationships rather than text. Windows and the Macintosh computer use a GUI.

GUI. See Graphical User Interface.

H

Hertz. See Frequency.

Home Networking. Connecting the different electronic devices in a household by way of a local area network (LAN).

Home Phoneline Networking Alliance. An association of companies who are working on a standard for home phoneline networking. HomePNA technology allows plug-and-play networking through the use of existing telephone wiring.

HomePNA. See Home Phoneline Networking Alliance.

HomeRF. Also known as Home Radio Frequency Working Group. An industry specification for the interaction of wireless digital communication between PCs and electronic devices in the home.

HTML. See Hypertext Markup Language.

HTTP. See Hypertext Transfer Protocol.

Hub. The point on a network where circuits are connected.

Hybrid Fiber/Coax (HFC). A type of network architecture that includes a combination of coaxial and fiber cables to distribute signals to a group of individual locations (typically 500 or more).

Hypertext. Documents or other information with embedded links that enable a reader to access tangential information at specific points in the text.

Hypertext Markup Language (HTML). The computer language used to create hypertext documents, allowing connections from one document or Internet page to numerous others. HTML is the primary language used to create pages on the World Wide Web.

Hypertext Transfer Protocol (HTTP). The transport protocol in transmitting hypertext documents around the Internet. The first part of an address (URL) of a site on the Internet, signifying the document is written in Hypertext Markup Language (HTML).

Hz. See Frequency.

I

IDSL. See ISDN Digital Subscriber Line.

IEEE. See Institute of Electrical and Electronics Engineers.

Institute of Electrical and Electronics Engineers (IEEE). A membership organization comprised of engineers, scientists, and students that sets standards for computers and communications.

Integrated Services Digital Network (ISDN). A circuit-switched communication network, closely associated with the public switched telephone network, that allows dial-up digital communication at speeds up to 128 Kilobits per second.

International Organization of Standardization (ISO). Develops, coordinates, and promulgates international standards that facilitate world trade.

International Telecommunication Union (ITU). A United Nations organization that coordinates use of the electromagnetic spectrum and creation of technical standards for telecommunication and radio communication equipment.

International Telecommunication Union/Telecommunication Standardization Sector (ITU-T). The branch of the ITU that is responsible for telecommunication standardization.

Internet Engineering Task Force (IETF). The standards organization that standardizes most Internet communication protocols, including Internet protocol (IP) and hypertext transfer protocol (HTTP).

IETF. See Internet Engineering Task Force.

I**nternet Protocol (IP).** The standard signaling method used for all communication over the Internet.

Internet Service Provider (ISP). An organization offering and providing Internet access to the public using computer servers connected directly to the Internet. For information on Internet Service Providers who offer DSL in your area, visit the DSL Lookup Service.

Intranet. A network serving a single organization or site that is modeled after the Internet, allowing users access to almost any information available on the network. Unlike the Internet, Intranets are typically limited to one organization or one site, with little or no access to outside users.

IP. See Internet Protocol.

IP Address. A numeric identifier for your computer. Just as the post office delivers mail to your home address, servers know to deliver data to your computer based on your IP address. IP addresses can be dynamic, meaning that your computer “borrows” the IP address for the necessary timeframe, or they can be fixed, meaning that the number solely belongs to your computer.

ISDN. See Integrated Services Digital Network.

ISO. See International Organization of Standardization.

ISP. See Internet Service Provider.

ITU. See International Telecommunication Union.

ITU - T. See International Telecommunication Union/Telecommunication Standardization Sector.

IXC. See Interexchange Carrier.

J

JPEG. See Joint Photographic Experts Group.

Joint Photographic Experts Group (JPEG). A committee formed by the International Organization of Standardization to set standards for digital compression of still images. Also refers to the digital compression standard for still images created by this group.

K

Kbps. Kilobits per second.

Kilobit. One thousand bits. See also Bit.

Kilobyte. One thousand bytes. See also Byte.

L

Laser. From the acronym for "Light Amplification by Stimulated Emission of Radiation." A laser usually consists of a light-amplifying medium placed between two mirrors. Light not perfectly aligned with the mirrors escapes out the sides, but light perfectly aligned will be amplified. One mirror is made partially transparent. The result is an amplified beam of light that emerges through the partially transparent mirror.

Last Mile. See Local Loop.

Local Area Network (LAN). A network connecting a number of computers to each other or to a central server so that the computers can share programs and files.

LAN. See Local Area Network.

LLC Encapsulation. See Logical Link Control Encapsulation

Logical Link Control (LLC) Encapsulation. A data link-level transmission control mechanism that involves the use of a logical link control header that identifies the protocol being carried. This allows the end device(s) to properly decipher the Protocol Data Unit (PDU). This is accomplished by prefixing the PDU by an IEEE 802.2 LLC header.

Local Loop. The copper lines between a customer's premises and a telephone company's telephone exchange.

M

MAC Address. See Media Access Control Address.

Mbps. Megabits per second.

Media Access Control Address. A hardware address that has been embedded into the network interface card (NIC) by its vendor to uniquely identify each node, or point of connection, of a network.

Megabit. One million bits.

Megabyte. 1,000,000 bytes, or 1,000 kilobytes. See Byte.

Microcell. A bounded physical space in which a number of wireless devices can communicate

Millions of Instructions Per Second (MIPS). A common measure of the speed of a computer processor.

Modem (MOdulator-DEModulator). A device that converts digital data into analog signals and vice-versa for transmission over a telephone or cable line.

Moving Pictures Experts Group (MPEG). A committee formed by the International Standards Organization to set standards for digital compression of full-motion video. Also stands for the digital compression standard created by this committee.

MPEG-1. An international standard for the digital compression of VHS-quality, full-motion video.

MPEG-2. An international standard for the digital compression of broadcast-quality, full-motion video.

Multicast. The transmission of information over the Internet to two or more users at the same time.

Multiplexing. Transmitting multiple signals over a single communications line or computer channel. The two common multiplexing techniques are frequency division multiplexing, which separates signals by modulating the data onto different carrier frequencies, and time division multiplexing, which separates signals by interleaving bits one after the other.

N

NAP. See Network Access Provider.

Narrowband. A designation of bandwidth less than 56 Kilobits per second.

Narrowband ISDN. See ISDN.

NAT. See Network Address Translation.

NetBIOS. The basic input/output system of the Internet.

Network Access Provider (NAP). Another name for a provider of networked telephone and associated services, usually in the U.S.

Network Address Translation (NAT). Network Address Translation (NAT) enables a local area network (LAN) to use one set of IP addresses for internal traffic and a second set of IP addresses for external traffic. This feature is used by the system so an end user can have an internal computer network in their home, with all its computers using internal IP addresses, using only one routable IP address, which accesses the outside (Internet).

Network Interface Card (NIC). A card that connects a workstation to a local area network.

Network Service Provider (NSP). A high-level Internet provider that offers high-speed backbone services.

Network Telephone Adapter. A class of electronic device that transmits and receives telephone conversation digitally through some types of packet network. One or more telephones are connected to the adapter in order to carry out verbal conversation.

Network Termination Equipment (NTE). The equipment at the ends of the communication path.

NIC. See Network Interface Card.

N-ISDN. See Narrowband ISDN.

NSP. See Network Service Provider.

NTE. See Network Termination Equipment.

O

OC-3. See Optical Carrier 3.

ONU. See Optical Network Unit.

Optical Carrier 3 (OC-3). An fiber optic line carrying 155 Megabits per second; a U.S. designation generally recognized throughout the telecommunications community worldwide.

Optical Network Unit (ONU). A form of access node that converts optical signals transmitted via fiber to electrical signals that can be transmitted via coaxial cable or twisted pair copper wiring to individual subscribers. See Hybrid Fiber/Coax.

P

Packet-switched Network. A network that allows a message to be broken into small "packets" of data that are sent separately by a source to the destination. The packets may travel different paths and arrive at different times, with the destination sites reassembling them into the original message. Packet switching is used in most computer networks because it allows a very large amount of information to be transmitted through a limited bandwidth.

Passive Optical Network (PON). A fiber-based transmission network containing no active electronics.

Peripheral. An electronic device, such as a printer or scanner, that is not integral to running a computer, but increases the capabilities of PCs.

Plain Old Telephone Service (POTS). An acronym identifying the traditional function of a telephone network to allow voice communication between two people across a distance. In most contexts, POTS is synonymous with the public switched telephone network (PSTN).

Point of Presence (POP). The physical point of connection between a data network and a telephone network.

Point-to-Point Protocol (PPP). Point-to-Point Protocol is a protocol which allows a computer to access the Internet using a dial-up phone line and a high-speed modem. This can be accomplished over Ethernet (PPPoE), or over Asynchronous Transfer Mode (ATM; PPPoA).

PON. See Passive Optical Network.

POP. See Point of Presence.

POTS. See Plain Old Telephone Service.

POTS Splitter. A device that uses filters to separate voice from data signals when they are to be carried on the same phone line, required for several types of DSL service.

Powerline Networking. A type of local networking that uses existing power lines within the office.

PPPoA. Point to Point Protocol over ATM. See Point to Point Protocol.

PPPoE. Point to Point Protocol over Ethernet. See Point to Point Protocol.

Private Branch eXchange (PBX). A private phone switching system used within a company that connects telephones to each other, allowing users to make inter-office as well as outbound telephone calls. Most companies now use a digital PBX switching system that utilize digital telephones, and includes features such as voicemail, call management, and caller ID.

PRI-ISDN. See Primary-rate ISDN.

Primary-rate ISDN (PRI-ISDN). The primary rate ISDN interface provides 23-64 Kilobits per second channels (called B channels) to carry voice or data and one 16 Kilobits per second signaling channel (the D channel) for call information.

Public Switched Telephone Network (PSTN). The worldwide communications network that carries phone calls and data.

R

Radio Frequency (RF). Electromagnetic carrier waves upon which audio, video, or data signals can be superimposed for transmission.

RADSL. See Rate-Adaptive Asymmetric Digital Subscriber Line.

Rate-adaptive Digital Subscriber Line (RADSL). A variation of DSL that uses carrierless amplitude phase modulation, divides the available frequencies into discrete sub-channels and also maximizes performance by adjusting the transmission to the quality of the phone line while in use.

Residential Gateway. A device that allows multiple devices access to the Internet through one single high-speed Internet connection.

RF. See Radio Frequency.

Request for Comment (RFC) 1483. RFC 1483 was developed to allow the successful transmission of multiple protocols over ATM networks. This RFC is broken down into two methods of implementation; VC based multiplexing and LLC encapsulation. The breakdown on both are mentioned below.

RJ-45 Plug. Short for Registered Jack-45, the RJ-45 is an eight-wire plug used to connect computers onto a local area network (LAN), especially Ethernet.

Roaming. Movement of a wireless node between two microcells.

Router. The central switching device in a packet-switched computer network that directs and controls the flow of data through the network.

S

SCSI. See Small Computer System Interface.

Small Computer System Interface (SCSI). A type of interface between computers and peripherals that allows faster communication than most other interface standards, often used to connect PCs to external disk drives.

Splitter. 1. For networking applications, a splitter is a device that splits a connection for use by two distinct outputs. 2. For DSL applications, a splitter is a device that sits on the outside of a residence that splits out the voice and data frequencies on the incoming phone line.

Splitterless. A DSL installation that does not use a splitter.

Switch. A device that selects paths or circuits. Routers are smart switches.

Symmetric Digital Subscriber Line (SDSL). A DSL technology that provides a maximum bandwidth of 1.5 Megabits per second using one phone line, with a downstream transmission rate that equals the upstream transmission rate, and that allows use of POTS service on the same phone line. Contrast with Asymmetric Digital Subscriber Line.

T

T141. The American National Standards Institute (ANSI) standard for asymmetric digital subscriber line using discrete multitone modulation, which the full-rate ADSL/G.dmt standard is based on.

TCP. See Transmission Control Protocol/Internet Protocol.

TCP/IP. See Transmission Control Protocol/Internet Protocol.

Telephone Exchange. A telephone company facility that handles the switching of telephone calls on the public switched telephone network (PSTN) for a small regional area.

Terabyte. 1,000,000,000,000 bytes, or 1,000 gigabytes. See Byte.

Time Division Multiplexing (TDM). A digital data transmission method that takes signals from multiple sources, divides them into pieces which are then placed periodically into time slots, transmits them down a single path and reassembles the time slots back into multiple signals on the remote end of the transmission.

Token Ring. A ring-like type of local area network whereby a "token" is passed to the workstations within the network.

Transmission Control Protocol/Internet Protocol (TCP/IP). A method of packet-switched data transmission used on the Internet. The protocol specifies the manner in which a signal is divided into parts, as well as the manner in which "address" information is added to each packet to ensure that it reaches its destination and can be reassembled into the original message.

Twisted Pair. The set of two copper wires used to connect a telephone customer with a switching office, loosely wrapped around each other to minimize interference from other twisted pairs in the same bundle. Synonymous with 2-wire line.

U

UDP. See User Datagram Protocol.

Uniform Resource Locator (URL). A text-based address used to identify specific resources on the Internet, such as web pages. URLs are arranged in a hierarchical form that specifies the name of the server on which a resource is located (such as www.bt.com) and the name of the file on that server (www.bt.com/index.html).

Universal Serial Bus (USB). A computer interface used for connecting computer peripherals such as printers, keyboards and scanners.

URL. See Uniform Resource Locator.

USB. See Universal Serial Bus.

User Datagram Protocol. A TCP/IP protocol describing how data packets reach application programs within a destination computer.

V

Variable Bit Rate (VBR). A data transmission that can be represented by an irregular grouping of bits or cell payloads followed by unused bits or cell payloads.

VDSL. See Very High Bit-rate Digital Subscriber Line.

Very High Bit-rate Digital Subscriber Line (VDSL). A type of asymmetric DSL that delivers from 13 to 52 Megabits per second downstream bandwidth and 1.5 to 2.3 Megabits per second upstream.

Video on Demand (VOD). A pay-per-view television service in which a viewer can order a program from a menu and have it delivered instantly to the television set, typically with the ability to pause, rewind, etc.

Virtual Reality Markup Language (VRML). A computer language that provides a three-dimensional environment for traditional Internet browsers, resulting in a simple form of virtual reality available over the Internet.

VOD. See Video on Demand.

VRML. See Virtual Reality Markup Language.

W

WAN. See Wide Area Network.

Wide Area Network (WAN). A network that interconnects geographically-distributed computers or local area networks.

Wireless. Transmission of data over radio waves rather than wiring. For more information on wireless, visit the Local Networking Resource Center.

Wireless Node. A user computer with a wireless network interface card.

X

xDSL. See DSL.

Numeric

802.3. An IEEE specification for CDMA/CD based Ethernet networks.

802.11. A family of IEEE specifications for 1 and 2 Megabits per second (Mbps) wireless Local Area Networks (LANs)

802.11b. An IEEE specification for 5.5 or 11 Megabits per second (Mbps) wireless Local Area Networks (LANs)

Regulatory Information

Declaration of Conformance with European Community Directive 1999/5/EC

This product is intended for use within the UK for connection to the public telephone network and compatible switchboards. This equipment complies with the essential requirements for the Radio Equipment and Telecommunications Terminal Equipment Directive 1999/5/EC. The Declaration of Conformance for the Intelligent Gateway is published on the following web site: http://www.2wire.com/about/declaration/UK.